



DTF1.1 – Reference Models for a European Multi-service Access Network

Peter Adams
BT
peter.f.adams@bt.com

Identifier	Deliverable DTF1.1
Class	Report
Version	06
Version Date	09/01/2006
Distribution	Public
Responsible Partner	BT
Filename	TF1_0010_V00_Muse_ref_models.doc

DOCUMENT INFORMATION

<i>Project ref. No.</i>	IST-6thFP-507295
<i>Project acronym</i>	MUSE
<i>Project full title</i>	Multi-Service Access Everywhere
<i>Security (distribution level)</i>	Public
<i>Contractual delivery date</i>	31 st December 2004 (re-planned to 30 th June 2005)
<i>Actual delivery date</i>	30 th June 2005, Issue 2: 09 th January 2006
<i>Deliverable number</i>	D TF1.1
<i>Deliverable name</i>	Reference Models for a European Multi-service Access Network
<i>Type</i>	Report
<i>Status & version</i>	V06
<i>Number of pages</i>	51
<i>WP/TF contributing</i>	TF1
<i>WP/TF responsible</i>	FT
<i>Main contributors</i>	See List of Contributors
<i>Editor(s)</i>	Peter Adams (BT),
<i>EU Project Officer</i>	Pertti Jauhiainen
<i>Keywords</i>	Architecture, Data Plane, Control Plane, Management Plane, Interfaces
<i>Abstract (for dissemination)</i>	The MUSE multi-service, multi-edge, broadband access architecture is outlined and reference models and open interfaces are described.

LIST OF CONTRIBUTORS

Peter Adams	BT
Benoit De Vos	ALCB
François Fedricx	ALCB
Hans Mickelsson	EABS
Frédéric Jounay	FT
Karsten Oberle	ALCS
Arnoud van Neerbos	TNO
Michel Borgne	FT
Govinda Rajan	LUNL
Antonio Gamelas	PTI
Sandro Krauss	DT
Tim Stevens	IME
Alex De Smedt	THOB

DOCUMENT HISTORY

Version	Date	Comments and actions	Status
V01	16-06-2005	Draft based on Version 7.2 of MA2.10 Part C	Open for review
V02	30-06-2005	Feedback added from Muenchen consortium meeting from: Hans Mickelsson, EABS Arnoud van Neerbos, TNO Karsten Oberle, ALCS Govinda Rajan, LUNL Tim Stevens, IME and corrections and changes from internal review.	Final
V03	29-10-2005	Draft of Issue 2	Open for task force review
V04	25-11-2005	Initial feedback from task force participants implemented.	Open for task force review
V05	14-12-2005	Feedback from task force review implemented Final draft of Issue 2	Open for internal review
V06	9-1-2006	Feedback from internal review implemented.	Final

TABLE OF CONTENTS

DOCUMENT INFORMATION	2
LIST OF CONTRIBUTORS	3
DOCUMENT HISTORY	4
TABLE OF CONTENTS	5
LIST OF FIGURES	7
ABBREVIATIONS	8
REFERENCES	10
EXECUTIVE SUMMARY	11
1 INTRODUCTION	12
2 ARCHITECTURAL OVERVIEW	12
2.1 Business roles	14
2.2 Network Nodes	15
2.3 Network Models	17
2.3.1 <i>Ethernet Network Model</i>	19
2.3.2 <i>IP Network Model</i>	20
2.4 Reference Models	20
2.4.1 <i>Data Plane</i>	21
2.4.2 <i>Management</i>	21
2.4.3 <i>Control</i>	22
3 INTERFACES	23
3.1 Data Plane Interfaces	23
3.1.1 <i>Network Termination 1 to Network Termination 2 Interface (T)</i>	24
3.1.2 <i>Access (Edge) Node to CPG Interface (U)</i>	24
3.1.2.1 <i>L1 of the U Interface</i>	24
3.1.2.2 <i>L2 U Interfaces</i>	25
3.1.2.3 <i>MUSE Ethernet U Interface Options</i>	26
3.1.2.4 <i>Muse IP Network Model U Interface Options</i>	28
3.1.3 <i>Access Node to Access Edge Node Interface (V')</i>	34
3.1.4 <i>Access Edge Node to Regional Network Interface (V) or Regional Network to Service Edge Node (A10)</i>	34
3.1.4.1 <i>V and A10 Interfaces for PPP Wholesale Model</i>	34
3.1.4.2 <i>V and A10 Interfaces for the IP Wholesale Model</i>	35
3.1.4.3 <i>V and A10 Interfaces for the L2 Wholesale Model</i>	37

3.2	Management Interfaces	38
3.2.1	Connectivity Provider to Access Network Manager Interface (Q_A)	39
3.2.2	Connectivity Provider to Regional Network Manager Interface (Q_R)	39
3.2.3	Connectivity Provider to Service Edge Node Interface (Q_S)	39
3.2.4	Connectivity Provider (ACS) to CPG Interface (Q_C)	39
3.2.5	Packager/NSP/ASP interface to Connectivity Provider (ACS) (Q_p)	40
3.3	Control Interfaces	41
3.3.1	CPE to AMF Interface (e1)	41
3.3.2	AMF – UAAF Interface (a3)	41
3.3.3	AMF – NACF Interface (a1)	42
3.3.4	NACF – CLF Interface (a2)	43
3.3.5	UAAF – CLF Interface (a4)	43
3.3.6	CLF and RACF Interface (e4)	43
3.3.7	CLF and AF Interface (e2)	44
3.3.8	UAAF to UAAF-proxy Interface (e5)	44
3.3.9	AAA and IP Address Assignment Protocols	44
3.3.10	CPG to Multicast Control Functions Interfaces (C_{m1} , C_{m2} and C_{m3})	44
3.3.11	AF to SPDF (G_q)	47
3.3.12	SPDF to A-RACF (R_q)	48
3.3.12.1	Information exchanged via the R_q interface	48
3.3.13	SPDF to BGF (I_a) Interface	49
3.3.14	A-RACF to RCEF (R_e)	50
3.3.15	A-RACF to RCEF _a (R_a)	50
4	Conclusion	51

LIST OF FIGURES

Figure 1: Reference Network and Business Role Domain Model	13
Figure 2: Functional basis of Ethernet network model	19
Figure 3: Functional basis of the IP network model	20
Figure 4: Data Plane Reference Points.....	21
Figure 5: Management Plane Reference Points	22
Figure 6: Control Plane Reference Points.....	23
Figure 7: An Example of Protocol Stacks for the MUSE Ethernet Model.....	24
Figure 8: Intelligent bridging (residential users)	26
Figure 9: Cross-connecting (residential users).....	27
Figure 10: Business users in the Ethernet Network Model	27
Figure 11: U-Interface Protocol Stack	28
Figure 12: L2 switching of IPoPPPoE traffic.....	29
Figure 13: PPPoE relay.....	29
Figure 14: Protocol Stack for Relaying PPP Traffic in the Access Node.....	29
Figure 15: IPoPPPoE traffic handled in IP forwarder (LAC/PTA).....	30
Figure 16: Protocol Stack for L2TP Access Aggregation (LAC).....	30
Figure 17: Protocol Stack for PPP Terminated Aggregation (PTA).....	30
Figure 18: Data plane example for the basic scenario with NAP providing IP services	31
Figure 19: U Interface Protocol Stack for NAP Provided IP Services	32
Figure 20: Most applicable business scenario for routed IP in the NAP network.....	33
Figure 21: U-Interface Protocol Stack for Routed IP in the NAP Network.....	33
Figure 22: V'- Interface Protocol Stack for IPoE.....	34
Figure 23: PPP Wholesale	35
Figure 24: V/A10 Interface Protocol Stack for PPP Wholesale Model	35
Figure 25: IP Wholesale Model	36
Figure 26: V/A10 Interface Protocol Stack for IP Wholesale Model	36
Figure 27: L2 Wholesale Model.....	37
Figure 28: V/A10 Interface Protocol Stack for L2 Wholesale Model	38
Figure 29: ACS to CPG Management Protocol Stack.....	40
Figure 30: One Step AAA process, DHCP Relay in the Access Network	45
Figure 31: Multicast Message Sequence	47

ABBREVIATIONS

3GPP	3rd Generation Partnership Project
AAA	Authentication, Authorization & Accounting
ACS	Auto-Configuration Server
ADSL	Asymmetric Digital Subscriber Line
AF	Application Function
AMF	Access Management Function
AN	Access Node
A-RACF	Access – Resource and Admission Control Function
ASP	Application Service Provider
ATM	Asynchronous Transfer Mode
BPON	Broadband Passive Optical Network
BRAS	Broadband Remote Access Server
C-BGF	Core – Border Gateway Function
CLF	Connectivity Session Location and Repository Function
CPE	Customer Premises Equipment
CPG	Customer Premise Gateway
CPN	Customer Premises Network
C-VLAN	Customer Virtual Local Area Network
DHCP	Dynamic Host Configuration Protocol
DSCP	Differentiated Services Code Point
DSL	Digital Subscriber Line
EAP	Extensible Authentication Protocol
ER	Edge Router
FCAPS	Fault, Configuration, Administration, Performance and Security
GPON	Gigabit-capable Passive Optical Network
HIS	High Speed Internet
IGMP	Internet Group Management Protocol
IMS	IP Multimedia Subsystem
IP	Internet Protocol
IP-CAN	IP-Connectivity Access Network
IPv4, IPv6	Internet Protocol version 4, Internet Protocol version 6
ISP	Internet Service Provider
MAC	Media Access Control
MPLS	Multi-protocol Label Switching
NACF	Network Access Configuration Function
NAP	Network Access Provider
NAPT	Network Address and Port Translator
NASS	Network Attachment Sub-System
NAT	Network Address Translator
NGN	Next Generation Network
NSP	Network Service Provider
PDBF	Profile Data Base Function
PIM	Protocol Independent Multicast
PIM DM	Protocol Independent Multicast Dense Mode
PON	Passive Optical Network
PPP	Point-to-Point Protocol
PPPoA	PPP over ATM
PPPoE	PPP over Ethernet
QoS	Quality of Service
RACS	Resource and Admission Control Sub-system
RADIUS	Remote Authentication Dial In User Service

RCEF	Resource Control Enforcement Function
RDB	Resource Data Base
RGW	Residential Gateway
RNP	Regional Network Provider
RPC	Remote Procedure Call
SIP	Session Initiation Protocol
SLA	Service Level Agreement
SPDF	Service-based Policy Decision Function
SSM	Source Specific Multicast
S-VLAN	Service Virtual Local Area Network
TISPAN	Telecoms & Internet converged Services & Protocols for Advanced Networks
TCP	Transmission Control Protocol
TMN	Telecommunication Management Network
UAAF	User Access Authorisation Function
UDP	User Datagram Protocol
VDSL	Very high speed Digital Subscriber Line
VLAN	Virtual Local Area Network

REFERENCES

- [1] DSL Forum TR-058, "Multi-Service Architecture & Framework Requirements", September 2003
- [2] MUSE deliverable DA2.2, "Network architecture and functional specifications for the multi-service access and edge", January 2005
- [3] Muse deliverable DA1.1, "Towards multi-service business models"
- [4] MUSE deliverable DB3.1, "Detailed Requirement-Based Functional Specification of Gateway"
- [5] MUSE deliverable DB1.1 "Access node specifications for service needs", Part III "Packet-to-Packet Gateway", January 2005
- [6] MUSE deliverable DB1.1 "Access node specifications for service needs", Part IV "TV-over-IP Head-End", January 2005
- [7] MUSE deliverable DTF3.2, "Detailed description of residential gateway and advanced features"
- [8] MUSE deliverable DTF1.3, "OAM and NSM Chain automation for multi-domain/multi-provider access networks", January 2005
- [9] DSL Forum TR-069, "CPE WAN Management Protocol", May 2004
- [10] NGN Functional Architecture; Resource and Admission Control Subsystem (RACS); Release 1, V1.5.0, December 2004
- [11] NGN Functional Architecture; Network Attachment Subsystem (NASS); Release 1, V0.4.0, May 2005
- [12] DSL Forum WT-101 v4, "Migration to Ethernet Based DSL Aggregation", November 2004
- [13] 3GPP 29.203
- [14] TISPAN_NGN Release 1: Release Definition, v040, March 2005

EXECUTIVE SUMMARY

This deliverable provides an overview of the MUSE architecture, defines reference models that map the functional architecture on to network nodes, and outlines the open interfaces required for a MUSE platform to simultaneously deliver multiple services to users from multiple service/application providers.

MUSE has devised two new business roles, extending the set established by the DSL Forum to better enable the multi-service multi-provider business model. The business roles are defined briefly and the deliverable then maps network nodes onto the business roles. The defining features of the network nodes are summarised.

The two MUSE network models that have been the focus of the architecture research are introduced and the top level innovative mechanisms for delivering multiple connections with quality of service between end users and multiple service/application providers are outlined.

Reference models for the data plane, management plane and control plane are presented in order to identify reference points which may form the basis of open interfaces. In the reference models the data transport, control and management functions needed in each business role domain are identified along communications paths between them. Each communication path may provide a reference point. If the reference point is between two business role domains then it will give rise to an open interface.

Finally the deliverable describes open interfaces in terms of the information flows across the interfaces and/or the protocols used.

There are a number of options in the MUSE architecture for delivering the required connectivity and quality of service, and for how the network elements are managed and controlled to obtain the delivery. The choice of options required to define a specific MUSE platform is conditional on the exact service mix, the regulatory and operational environment in each country and business processes preferred by the operating companies. Where possible recommendations are made in this document for the most appropriate choices in particular circumstances.

In the first issue of the deliverable some open issues were identified for further study. This issue incorporates the results of the further study, in particular the expansion of the control reference points and interfaces on AAA and IP address assignment to include the Network Assignment Sub-System (NASS) functions of TISPAN. In addition improvements have been made to the protocol stack diagrams of the data plane interface section to make them clearer.

1 INTRODUCTION

The MUSE project encompasses many different research topics under the umbrella of an architecture sub-project (SPA). There are also three subprojects (SPB, SPC, SPD) that focus on the specific deployment scenarios of migration, non-legacy and FTTx/xDSL respectively. This deliverable provides an overview of the reference models for a European Multi-service Access Network that draws on the output of all the subprojects. The different deployment scenarios mean that there will be a number of variants of the multi-service access platform resulting from the MUSE project. Indeed, there will also be variants arising from different architectural choices. In SPB value-add service enablers are described that provide functionality over and above the functionality required for L3 communications. These service enablers allow processing in the MUSE domain in support of multi-media communication, eg teleconferencing, transcoding, content marking. Value-add service enablers are not covered in this deliverable and will be described in a later MUSE deliverable. This document describes the reference models required to create a platform for delivering broadband access up to L3. In particular it describes the open interfaces between business role domains that are necessary to integrate a MUSE platform into end-to-end networks and to be able to manage it and control service sessions across it.

Section 2 of this deliverable gives an overview of the MUSE architecture and how it maps to the business role domains. The business models for delivering services are described and the top level mechanisms for delivering connections and quality of service are outlined.

Section 2 also identifies the small number of types of network node which connected together form a MUSE network platform. Nodes have a quasi-geographical positioning between the customer premises and the service/application provider domains. Two network models are then outlined which have been the focus of the architecture research.

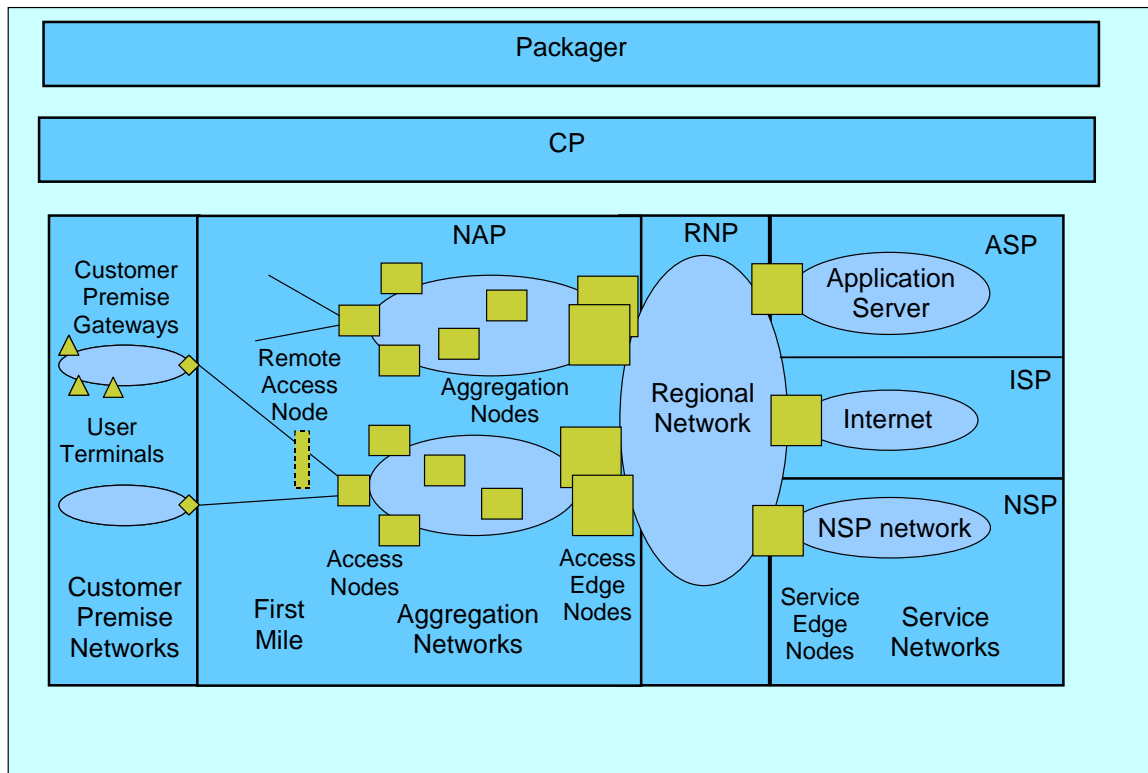
Finally in Section 2 reference models for the data plane, management plane and control plane are presented in order to identify reference points which may form the basis of open interfaces. In the reference models the data transport, control and management functions provided in each business role domain are identified along communications paths between them. Each communication path may provide a reference point. If the reference point is between two business role domains then it will give rise to an open interface.

Section 3 of the deliverable describes the open interfaces in terms of the information flows across the interfaces and/or the protocols used. Where these protocols are well established standards they are not described in detail. Interfaces between nodes in the same domain are sometimes mentioned where this aids understanding.

2 ARCHITECTURAL OVERVIEW

The definition of an access architecture is a central goal in MUSE to enable fulfilment of the overall mission statement *"to research and develop a future low-cost, full-service access and edge network, which enables the ubiquitous delivery of broadband services to every European citizen."* The architecture determines the totality of functions that comprise a MUSE platform and so to position what follows a top level architectural overview is helpful. In addition, it is necessary to understand the business role domains that are required to

deliver multi-service access. Fig.1 shows the network reference model and business role domains that have been established as the framework for the MUSE studies. The framework is based on the industry view developed by the DSL Forum [1]. This has, however, been extended to include two additional business roles: Packager and Connectivity Provider as defined in [2] and [3]. The scope of MUSE from a network perspective is primarily the access and aggregation network that is operated by the Network Access Provider (NAP). However, to address the overall provision and operation of multiple services to everywhere MUSE has also studied Residential Gateways (RGWs) [4] , Packet-to-Packet Gateways [5] and TVoIP Gateways [6] and the management and control functionalities that reside in the various business role domains. In this deliverable we will not be describing the RGWs or Service Edge Nodes, but the management and control functionalities form an important aspect of the overall description, particularly in the interfaces section.



Key: NAP = Network Access Provider ASP = Application Service Provider
 RNP = Regional Network Provider CP = Connectivity Provider
 NSP = Network Service Provider ISP = Internet Service Provider

Figure 1: Reference Network and Business Role Domain Model

2.1 Business roles

The business roles shown in Fig. 1 cover the main groups of business and operational functions required to deliver and sustain multi-service broadband access services. The one role that is not shown explicitly is that of Loop Provider. This role is needed to cover the case of local loop unbundling. However, this is an extension of the business model that is easily accommodated by the MUSE architecture. It does not materially affect the MUSE architecture or the open interfaces required and so will not be considered further in this document. The main business roles are:

Network Access Provider (NAP)¹

The NAP (also sometimes called Access Network Provider (ANP)) provides and operates the access and aggregation network between the end user's Customer Premise Gateway² (CPG) and (via the regional network) the NSPs, ISPs and ASPs. The NAP wholesales service connections to the NSPs and ASPs. Combined with the NSP the NAP may retail IP connections to end users.

Regional Network Provider (RNP)

The RNP provides and operates the regional network between the aggregation network and the NSPs, ISPs or ASPs. The regional network may not be present in all situations.

Network Service Provider (NSP)

The NSP provides (IP) addressing and connectivity to an IP network (ASP's equipment or the Internet) for end-users. If only Internet access is offered then the NSP is, more narrowly, referred to as an Internet Service Provider (ISP).

Application Service Provider (ASP)

The ASPs (and NSPs) trust a Packager who requests the Connectivity Provider to use the networks of NAPs and RNPs for access to users and configuration of their IP addresses. They keep profiles (for authentication and QoS control and management) of their users and offer applications for users via dedicated application servers.

Packager

The Packager role combines connection services obtained via the Connectivity Provider from NAPs, RNPs and NSPs with application services from one or more ASPs and offers this as a package to the customer. In general the Packager is technology agnostic (as such the Packager role does not include any service or network control and management functions, only business management functions – there will, of course, be management

¹ It became apparent in the generation of the first issue of this deliverable that it is sometimes the case that the provider of the access node and the provider of the aggregation network can be separate business entities. Re-examination of the business role model showed that it could encompass this case by assuming that all the aggregation was provided by the RNP with the NAP providing the Access Node.

² The term Customer Premise Gateway is intended to cover any group of functions that allow connection of CPE to the access network. In much of MUSE the focus has been the Residential Gateway which is a particular example of a CPG. Business premises may well have different gateways.

information flows between the Packager and other roles) and is the single point of contact for the customer. The Packager may also interface with other Packagers in order to provide “nomadism” services.

Connectivity Provider (CP)

The CP is responsible for obtaining end-to-end connectivity between the Customer Premise Equipment (CPE) and the NSP or ASP network, and guaranteeing the agreed QoS and security characteristics. The CP has Service Level Agreements (SLAs) with the NAP and the RNP regarding the required network resources. The CP can do the assignment of IP addresses to the CPE on behalf of the NSP or ASP. Furthermore, the CP may assemble billing information for network services and provide this to the Packager.

2.2 Network Nodes

Fig.1 also identifies the network nodes which connected together form a network platform. The nodes have a quasi-geographical positioning between the customer premises and the locations of the service/application providers. These locations are indicated below. It should be noted that a node is not the same as a single hardware entity (box) or a single software module. A node is a collection of co-located functions. The network nodes do not encompass all the functions required for a MUSE platform, only the network platform. There are functions for the management and control of the network platform that will be located elsewhere, eg management functions that are located in an element manager. The geographical location of these functions is not of importance for the platform although in a realisation of the platform the location may be governed by cost or efficiency considerations.

There are five different types of network node³:

- Access Node
- Remote Access Node
- Aggregation/Switching/Routing Node
- Access Edge Node
- Service Edge Node

Access Node (AN)

An Access Node is realized either as a DSLAM or an Optical Access Multiplexer. As a DSLAM it will contain DSL Line Terminations and possibly Feeder Line Terminations which could be optical or copper and provide connections to a Remote Access Node. As an Optical Access Multiplexer it contains Optical Line Terminations. The AN is located where the physical media of the access network converge and terminate. For the first mile copper access network this will be at the local exchange. For optical access it is possible that the point of convergence and termination is deeper into the network.

The AN node⁴ will contain:

³ The CPG can also be regarded as a node in the end to end network and, where appropriate, some indication of its functionality as it affects this deliverable is given. The CPG, however, contains functions that pertain to the Customer Premise Network which is not in the scope of this deliverable.

- bridging functions⁵ for L2
- aggregation functions at L1 and L2
- service enabler⁶ functions related to L1 and L2

The AN node may contain:

- routing/forwarding functions for L3
- switching functions for L2
- service enabler functions for L3 and above

Remote Access Node (Remote AN)

The Remote AN is either a subtended DSLAM, a Remote Access Multiplexer or an Optical Network Unit. It will contain Line Terminations which could be DSL or wireless. A Remote AN will be located between the customer premises and the AN. This will usually be between the customers' premises and the local exchange, the aim being to use short copper loops to operate higher rate DSL or possibly wireless technologies. This aim places requirements of lower cost (because of the smaller number of users served) and low power consumption (because of the increased difficulty of supplying power) on the realisation of a Remote AN. To achieve this Remote ANs may have a reduced functionality compared to ANs. The Remote AN will contain:

- bridging functions for L2
- aggregation functions at L1 and L2
- service enabler functions related to L1 and L2

The Remote AN may also contain switching functions for L2.

Aggregation/Switching/Routing Node (ASRN)

An ASRN contains aggregation and/or switching and/or routing functions depending on the network model (see Section 2.3). ASRNs will use specific L2 switching and aggregation technology, eg Ethernet, ATM. An ASRN can be located anywhere between the access node and the access edge node at points determined by the dimensioning of the aggregation network and the availability of equipment accommodation.

An ASRN may include:

⁴ As all the nodes will contain L1 termination functions they are not specific listed for each node.

⁵ Each of the functions listed for the nodes may include features that relate to the management and/or control of the functions.

⁶ A service enabler is a collection of functions that together enable a particular service, or feature of a service, to exist and to be controlled and managed. All the nodes in a network will contain service enabling functions relating to a number of service enablers. In the following chapters there are various functions mentioned that are located in the network nodes which are service enabling functions, eg the RCEF in the access edge node which is a Layer 3 service enabling function.

- protocol encapsulation, or translation, for circuit emulation across a aggregation node that uses a different L2 technology
- L3 routing
- service enabler functions for L2 and L3

Access Edge Node (AEN)

An (AEN) access edge node provides the interface between the aggregation network and the regional network. AENs will be placed in the network where interconnect to a regional network, or directly to a service edge node, is possible.

The AEN node will contain:

- bridging functions for L2
- aggregation functions at L2
- service enabler functions related to L1 and L2

The AEN node may contain:

- routing functions for L3
- switching functions for L2
- service enabler functions for L3 and above

Service Edge Node (SEN)

An SEN contains a gateway to a service platform. It terminates the regional network L1 and L2, and L3+ if appropriate, or is connected directly to an AEN. SENs are located at the service or application provider's premises.

A SEN provides:

- appropriate L1 and L2 interfaces to service platforms
- appropriate control and management interfaces to service platforms

and may provide L3 routing or termination functionality.

2.3 Network Models

The basis for the architecture is the general connectivity which is about providing correct forwarding of packets between a server and one or multiple hosts, or between multiple hosts themselves, based on L2 and/or L3 address information. There are different possibilities of connectivity wholesaling and retailing that a Network Access Provider (NAP) can offer to its customers. Three distinct business models have been identified which describe the possible roles of the providers NAP, NSP, ISP, ASP, Packager and CP. These are: PPP wholesaling, IP wholesaling and L2 wholesaling. These models impact the data plane interfaces and so are described in greater detail in section 3.1.3.

Connectivity is established by a combination of network management in the provisioning phase of service fulfilment and service and network control to enable a communications session. Part of this process is authentication and user IP address allocation. Authentication can be for network access and service/application usage. MUSE has identified a single step authentication and IP address allocation process which is described in section 3.3.

Whilst the architecture's primary aim is to provide point to point connectivity between the edge node and the CPG it also addresses the potential need for peer to peer connectivity and multicast connectivity for some applications. It was concluded that while business users require L2 peer to peer connectivity (e.g. for L2 VPN), there is no such requirement for residential users, which will then be connected at L3. Multicasting also poses specific choices and requirements as a connectivity model. Reference [2] describes how these connectivity requirements are provided in the architecture.

As well as providing connectivity the architecture is designed to enable the delivery of a specified Quality of Service (QoS) for each connection. QoS requirements are specified by bounds on a number of properties, eg bit rate, error rate, delay, jitter, lost packets. These properties arise from errors occurring in the underlying transmission systems as a result of interference, and/or bandwidth restrictions and the queues that are formed at aggregation, switching or routing nodes by the random arrival of packets. Transmission errors are minimised by the correct deployment of systems; bandwidth/queuing effects are minimised by appropriate network resource dimensioning and management and by usage control.

The resource management is based on pre-provisioned resources in the access network. The resources are organised by pre-configured "QoS pipes" running across the aggregation network. For each pipe, a certain bandwidth is reserved, and the network is configured such that the traffic entering the pipe will be delivered with a pre-defined QoS level, at least as long as the reserved bandwidth is not exceeded. Resource management is based on the principles of:

- Building a view of the network's static resources. The resources of the access network are controlled by a centralised function that has a view of all the resources of the network. This view is obtained from the various network elements managers that manage the access nodes, aggregation nodes and edge nodes.
- Building a view of the allocation of user's addresses. In order to identify the path taken by a flow the network resources management function, depending on the network architecture (L2, L3) may obtain from the AAA and IP address allocation functions the user's IP address, user's MAC address, selected NSP, originating access node, and the line to which the user is attached.

Usage control is based on the principles of:

- Building a view of the use of resources. For each link of a QoS pipe the current state of usage is maintained.

- Controlling the admission of new IP flows, or tearing down flows, per individual request. The network resource control function receives new connection QoS requests from the CP. Based on the real time view of the use of resources in the network, it is able to decide if a new individual QoS request can be accepted or not. If accepted then the individual flow is enabled in the network elements. There may also be cases in which the resource control can decide to tear down an existing flow.
- Policing and shaping in the network elements, either at the pipe level, the IP flow level, or the traffic class level.

MUSE has identified two network models which can deliver the connectivity and QoS control required for the business models: the Ethernet network model and the IP network model. In these models Remote ANs are not explicitly identified. This is because the models are primarily concerned with L2 and L3 functionality. For either model Remote ANs may be used and then some of the AN functionality at layer 2 is moved/extended into the RANs. L3 functionality in the IP network model would most likely not be moved to the Remote AN because the Remote ANs need for reduced complexity.

2.3.1 Ethernet Network Model

The Ethernet network model presented in Figure 2 can be considered as the network that has completely migrated to Ethernet. This means that there is Ethernet-based connectivity at L 2, from the subscriber up to the edge, for traffic in either IPoE or IPoPPPoE format⁷. The aggregation network may support MPLS over Ethernet.

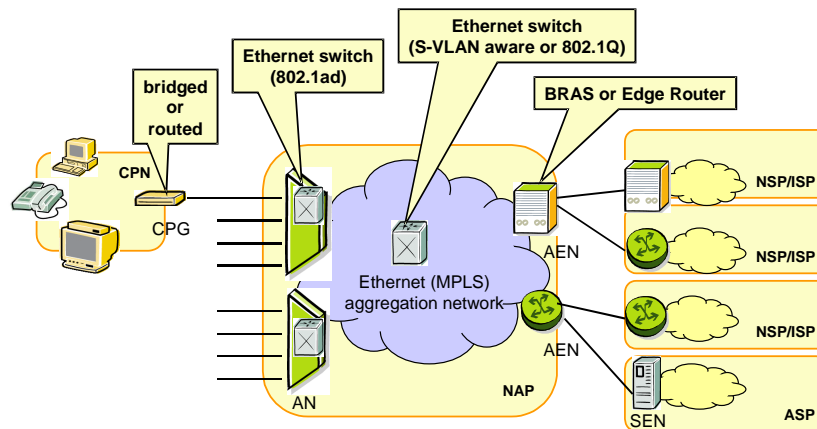


Figure 2: Functional basis of Ethernet network model

⁷ This does not preclude consideration of ATM in the first mile.

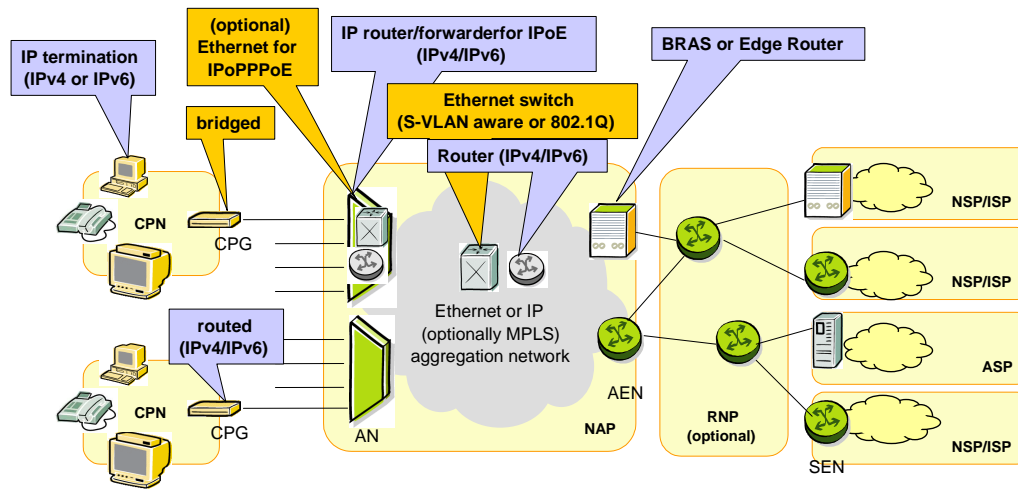


Figure 3: Functional basis of the IP network model

2.3.2 IP Network Model

Fig. 3 shows the functional basis of the IP network model. The network between the AN and the NSP edge node can be either an Ethernet or a routed IP network or a combination of both. Also the aggregation network may deploy MPLS, either over an Ethernet transport or another transport like PoS. In any case the access edge node will be an IP forwarder.

Note, that even if a routed IP network is used in the aggregation the NAP can still provide L2 services between the AN and the AEN, e.g. using L2TP or MPLS.

2.4 Reference Models

The intent of section 3 is to identify and describe the open interfaces required for the operation of a MUSE access and aggregation network. To define interfaces requires the drawing of a boundary around the functions that are implemented in a MUSE platform and possibly the identification of boundaries within MUSE as a consequence of different business entities owning different nodes. The current state of the definition of the MUSE architecture with various options for control and management, the multiplicity of business roles and the variation of regulatory environments make the definition of open interfaces multifaceted. However, a good first step is to identify reference models for the data, control and management planes and to identify reference points in these models that could be the location for the physical realisation of open interfaces.

This section describes three reference models for the MUSE architecture, one each for data, control and management, and identifies the reference points in each model. In each model the interconnections between functional elements are shown. Each interconnection leads to a reference point between functional entities. The exact placing of some functional elements, especially in the management and control planes, is an area of ongoing study in MUSE. If functional elements are moved between business role domains then, although

current reference points will remain, reference points which are not labelled in the diagrams at present will need to be. Those between business role domains will become open interfaces.

2.4.1 Data Plane

The data plane reference model in Fig. 4 contains those functional elements that provide the end-to-end service connection from the customer domain to the ASP or NSP domain, ie terminal, CPG, Remote⁸ AN, AN, ASRN(s), AEN, regional router(s), SEN and application server. In end user to end user applications, eg VoIP the service edge node will be interconnected across an IP core network to another service edge node and subsequent access and aggregation network. For this document we need only to consider the customer to application server part.

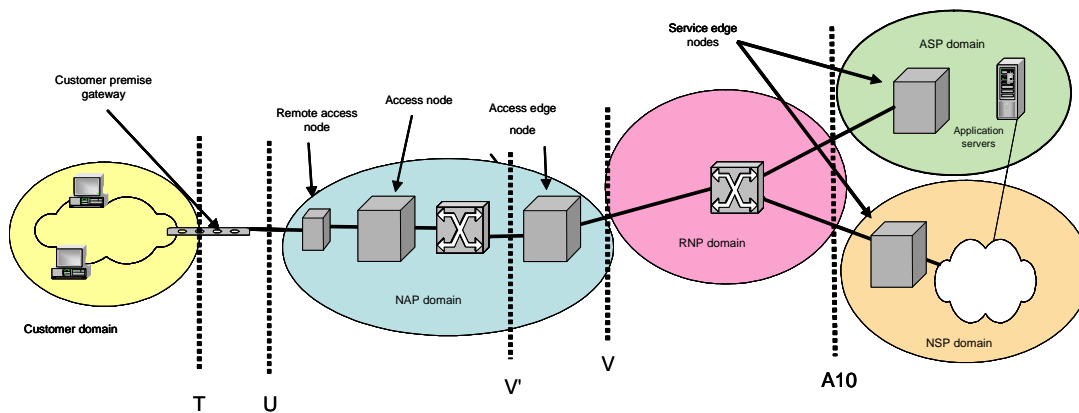


Figure 4: Data Plane Reference Points

The reference points of interest in this model are labelled T, U, V', V and A10. This terminology is taken from the reference architecture described by the DSL Forum [1] enhanced by the addition of the V' reference point. The V' reference point is of use when the aggregation is primarily provided by the regional network provider and the NAP provides only the AN (and maybe some local aggregation). The V reference point vanishes in some realisations where there is no regional network.

2.4.2 Management

Fig. 5 shows the management connections (the dotted lines) required to manage the elements in the MUSE architecture. Some of these connections use the data plane connections for communications, eg the ACS to CPG management connection, and others may use separate data plane connections, eg the connectivity manager to access network manager connection. The reference point labels use a combination of nomenclature drawn

⁸ The general case of inclusion of the Remote AN is shown. In many deployment situation there will not be a Remote AN

from TMN and other sources. Note that the reference points are logical reference points and can only lead to interfaces if associated with an appropriate data plane reference point and interface.

As described in section 2.3 the methodology for the delivery of QoS for each connection across the network involves building a view of the available resources and controlling the use of the network accordingly. This implies the existence of a database (or distributed databases) to record the network topology, total resources, uncommitted resources, and existing connections across the network. This resource database, shown as RDB in Fig. 5, needs to be updated by the access network manager with the details of the VLAN pipes in the Ethernet segments between the AN and AEN, as and when they are provisioned.

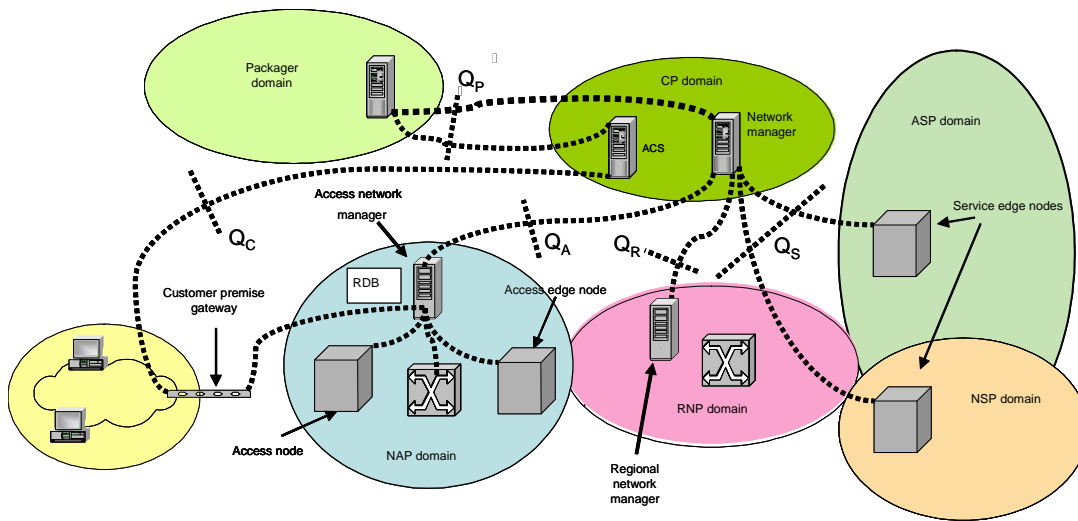


Figure 5: Management Plane Reference Points

2.4.3 Control

Fig. 6 shows the control connections (the dashed lines) required to control the elements in the MUSE architecture. All these connections will of necessity use the data plane connections for communications. However, some will be by dedicated control channels and others may be associated with a specific data plane connection. The reference point labels use a combination of nomenclature drawn from ETSI-TISPAN and other sources. Note that the reference points are logical reference points and can only lead to interfaces if associated with an appropriate data plane reference point and interface.

As mentioned in section 2.4.2 the RDB shown in Fig. 5 need to be updated with information about the connections across the network. This implies a control connection from the AAA functions to the database. It also implies a control connection from the A-RACF to the database for A-RACF to determine if resources are available for a particular IP flow to be allowed across the network and, when they are, to update the database with the resource usage information (and to reverse this when an IP flow ceases).

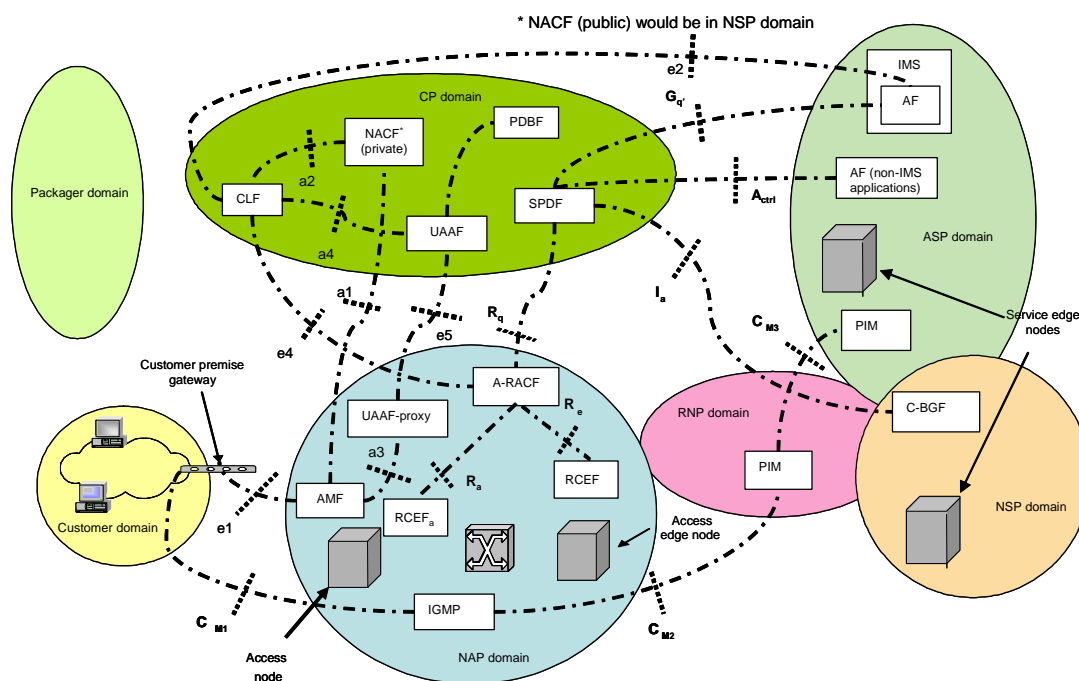


Figure 6: Control Plane Reference Points

3 INTERFACES

This section describes the open interfaces for each plane. A complete interface which allows the connection and interoperability of two functions contained in separate realisations will require a minimum of L1 and L2 data plane interfaces to support higher level interfaces for data transport, or control or management protocol messages across the interface. Many of the interfaces that follow are International Standards, or use protocols that are International Standards, and so will not be described in detail.

3.1 Data Plane Interfaces

Using the reference points defined in Fig. 4 the following data plane interfaces can be defined:

- Network Termination 1 to Network Termination 2 Interface (T)
- A(E)N to CPG Interface (U)
- AN to AEN Interface (V')
- AEN to Regional Network Interface (V) or Regional Network to SEN (A10)

To understand the data plane protocols that operate across these interfaces it is useful to look at the protocol stacks that are implemented in each of the nodes. Fig. 7 shows an example of the protocol stacks used at each of the nodes and the CPG⁹ for the case of the Ethernet aggregation network. The two networks (aggregation and regional are shown in a darker shade to indicate that these are not nodes but networks and would contain multiple aggregation, switching or routing nodes. The regional network has the IP layer shown as hatched to indicate that it may or may not be present depending on the nature of the regional network.

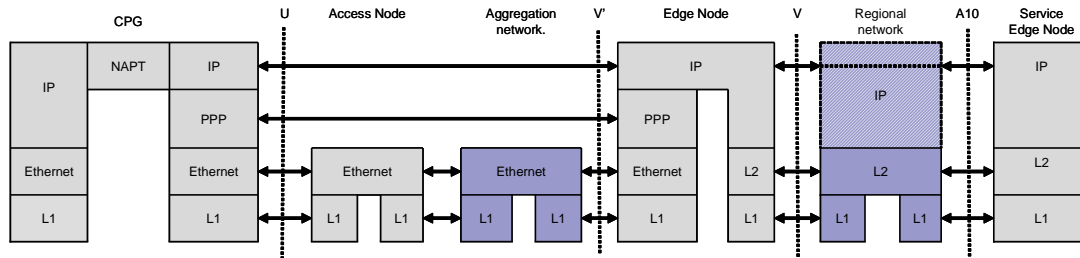


Figure 7: An Example of Protocol Stacks for the MUSE Ethernet Model

3.1.1 Network Termination 1 to Network Termination 2 Interface (T)

The T reference point in the MUSE architecture is usually assumed to be within the CPG. As such it does not make sense to define an open interface at the T reference point. However, further specification of the T reference point can be found in DTF3.2 “Residential Gateway and advanced features” [7]. More information on the functional architecture of the CPG may be found in MUSE deliverable [2].

3.1.2 Access (Edge) Node to CPG Interface (U)

The U reference point is the point at which CPGs, which may well be obtained by the customer from one of many suppliers, are connected to the Access Provider’s Network and so an open interface at this point is essential. The data plane interface is defined at L1 and L2, there being a number of options for each layer described in the MUSE architecture.

3.1.2.1 L1 of the U Interface

The L1 and physical characteristics of this interface are strongly media dependent, eg DSL, fibre, radio and this part of the document will point to various international standards to

⁹ The protocol stacks for the CPG are one of several options (see reference [7]). The variations within the CPG are not relevant to the discussion of interfaces here and so the example in Fig 7 will be used throughout this deliverable.

define this interface. The objective of the Table 1 is to give a rapid overview of some of the existing L1 technologies. It is a list that is subject to evolution with the emergence of new or disappearance of obsolete technologies respectively. In subproject D of MUSE research into advanced xDSL and FTTx technologies has been carried out that will contribute to this evolution.

Media	Technology	Reference to Standard
Twisted Pair	ADSL1, ADSL2(plus), ReADSL	ITU-T G.992.1, G.992.2, G992.3, G992.4, G992.5
	VDSL1, VDSL2	ITU-T G.993.1, G.993.2
	HDSL	ETSI and ITU
	SDSL	ITU
	SHDSL	ITU-T G.991.2,
	10Base-T	IEEE 802.3i
	100Base-T	IEEE 802.3u: Fast Ethernet
	Gigabit Ethernet	IEEE 802.3z/ab
Coaxial Cable	Cable modems	DOCSIS1.0, DOCSIS1.1, DOCSIS2.0, eDOCSIS
	10Base-5	IEEE 802.3 Thick Coax
	10Base-2	IEEE 802.3a Thin Coax
Point to Point Fiber	100BASE-L(B)X10	IEEE 802.3ah §58 Long Wavelength
	1000BASE-L(B)X10	IEEE 802.3ah §59 Long Wavelength
	10-Gigabit Ethernet	IEEE 802.3ae
Passive Optical Network	1000BASE-PX10(20)	IEEE 802.3ah §60 EPON
	Class A, B and C transceivers	ITU-T G.984.2 GPON BPON
Wireless	WLAN	IEEE 802.11
	WIMAX	IEEE802.16

Table 1: L1 Technologies

3.1.2.2 L2 U Interfaces

The L1 standards often include definition of the L2, eg ATM over DSL. However, the MUSE architecture focuses on Ethernet as the L2 protocol of choice for this interface, and so this section contains details of the options discussed earlier in this document and in DA2.2.

Although there may be a long term convergence on an end-to-end Ethernet L2 in the access and aggregation network a variety of L2 data protocols will coexist for a number of years. It is therefore useful to refer to these L2 protocols in this section.

- ATM (DSL forum TR-25)
- ETHERNET MAC (IEEE 802.3)
- GEM (GPON encapsulation Mechanism as described into ITU-T G.984.3)
- Token Ring (IEEE 802.5)
- FDDI Fiber Distributed Data Interface
- Layer 2 Protocol of X.25

- Layer 2 Protocol of Frame relay
- Layer 2 Protocol of ISDN Integrated Services Digital Network

3.1.2.3 MUSE Ethernet U Interface Options

The Ethernet network model presented in Fig. 2 can be considered as the network that has completely migrated to Ethernet. This means that there is Ethernet-based connectivity at L2 from the subscriber up to the edge, for traffic in either IPoE or IPoPPPoE format.

There are 3 options defined in MUSE for the way Ethernet is used in the AN:

- Intelligent bridging (residential users), shown in Fig. 8 where the connectivity in the AN is based on the MAC addresses, as in an ordinary Ethernet switch but the AN has additional intelligence for security, traffic management and accounting.

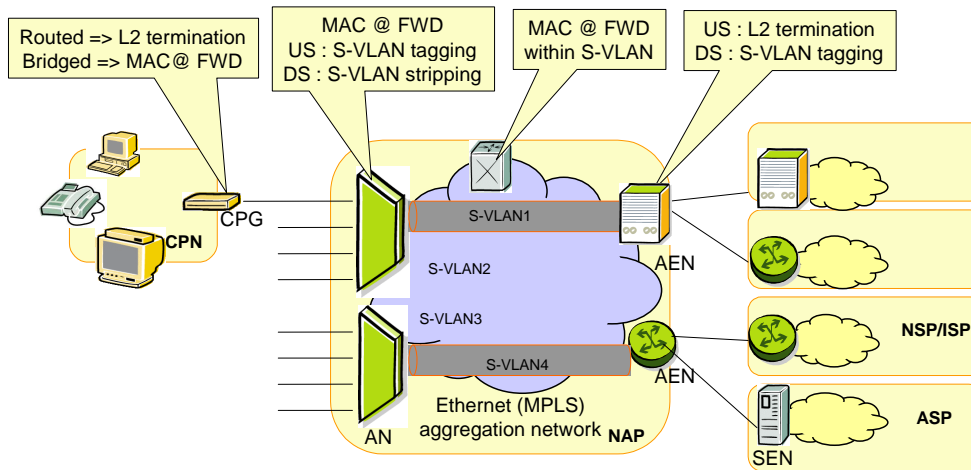


Figure 8: Intelligent bridging (residential users)

- Cross-connecting (residential users), shown in Fig.9, where the connectivity at the AN is based on VLAN-IDs, namely by associating one individual VLAN-ID to every end-user (i.e. to every line aggregated in the AN). The AN then behaves as a cross-connect, switching ports via the VLAN-IDs for connectivity in the downstream direction, and switching upstream traffic to the uplink.
- Business users, shown in Fig. 10, where it is recommended to use the S-VLAN tag. These users will generate 802.1Q-tagged Ethernet frames, and expect them to be transported transparently across the network to one or multiple other business locations (L2 VPN). In the ANs, the upstream frames are transparently sent and tagged with the corresponding S-VLAN (based on the line), and the downstream frames are transparently sent (after stripping the S-VLAN tag) to the line

corresponding to the S-VID. This approach can be combined with the bridged model and with the cross-connect model. In both cases some S-VLANs must be reserved in the network for business users only.

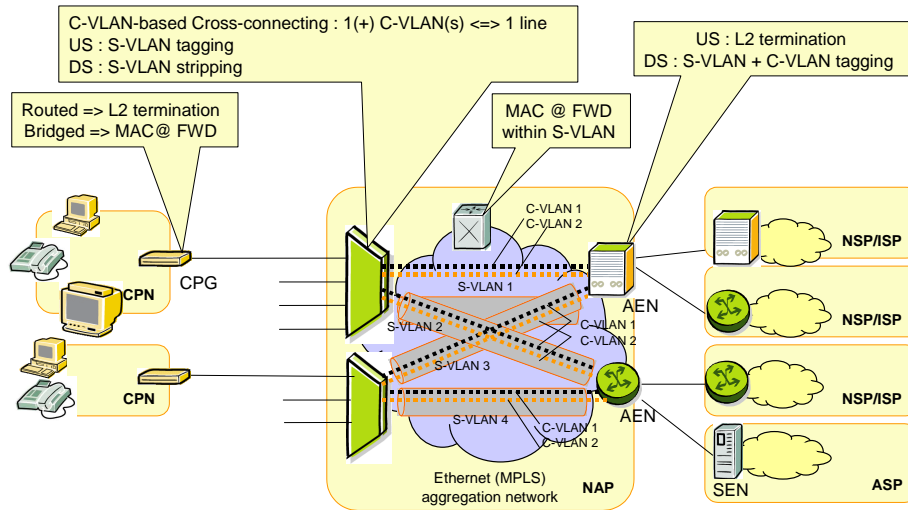


Figure 9: Cross-connecting (residential users)

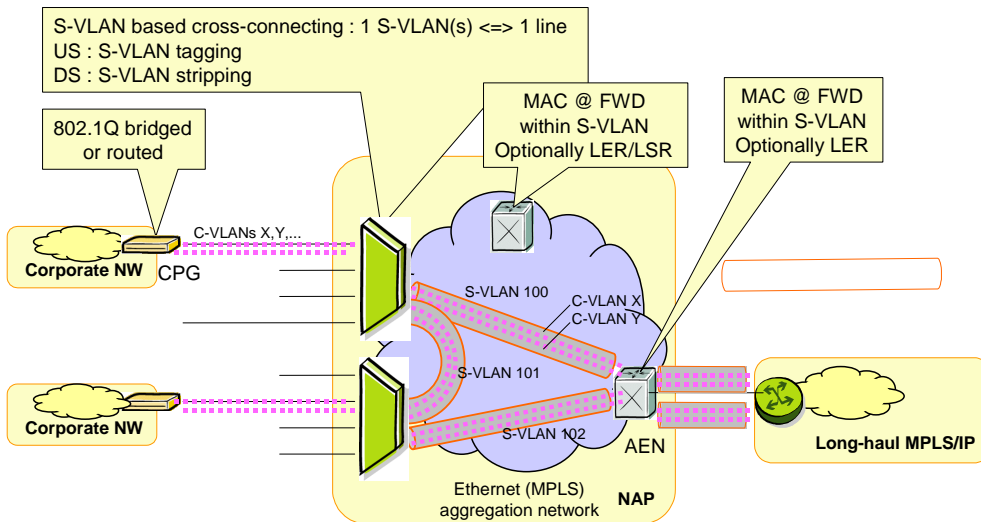
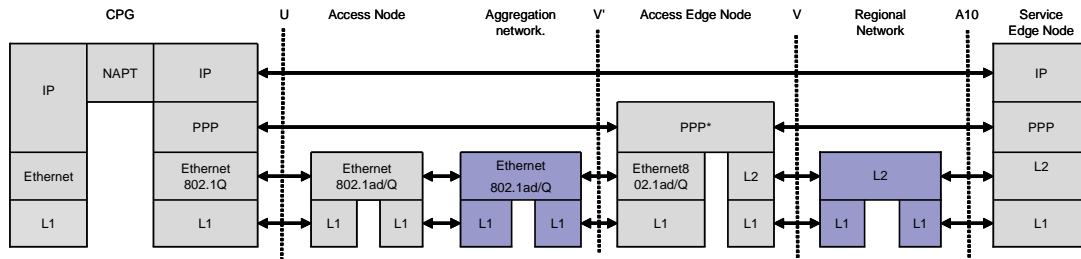


Figure 10: Business users in the Ethernet Network Model

In the first two options there is no difference in the protocol stack (Fig. 11) used across the U-interface. For the business user case, however, the frames are C-VLAN tagged.



* PPP session is either terminated in the Access Edge Node or tunnelled to the Service Edge node

Figure 11: U-Interface Protocol Stack

3.1.2.4 Muse IP Network Model U Interface Options

Fig. 3 shows the functional basis of the IP network model. The aggregation network between the AN and the NSP edge node can be either an Ethernet or a routed IP network or a combination of both. Also the aggregation network may deploy MPLS, either over an Ethernet transport or another transport like PoS. In any case the NSP edge node will be an IP forwarder.

An IP network model is characterized by IP forwarders which are deployed in the access and aggregation network and which completely terminate the L2 between the user and the network side ports while the IP traffic is forwarded between the ports.

Note, that even if a routed IP network is used in the aggregation the NAP can still provide L2 services between the AN and the reference point A10, e.g. using L2TP or MPLS.

Three scenarios were retained to handle IPoPPPoE traffic: transparent L2 switching, PPP relaying, processing PPP sessions.

Transparent L2 Switching

The first option to handle (IPo)PPPoE, shown in Fig. 12, is to keep the PPP termination point at the same place as in the Ethernet Network Model. This implies that the AN should switch this traffic transparently at L2 towards the AEN, where it will then either be terminated (IP wholesale) or tunnelled towards the NSP (PPP wholesale via L2TP). The protocol stack is the same as in Fig. 11.

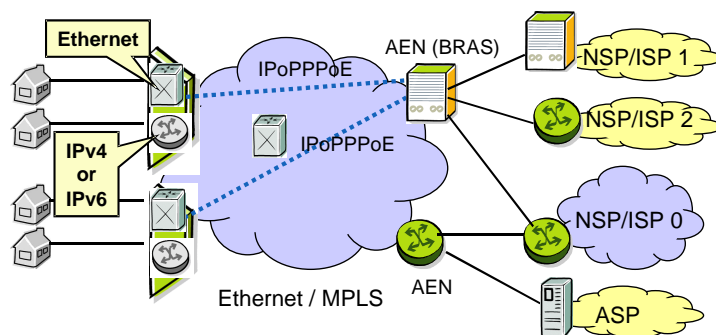


Figure 12: L2 switching of IPoPPPoE traffic

PPP Relaying

A more secure second option, shown in Fig. 13, consists of relaying the PPP traffic in the AN. This allows terminating L2 for PPPoE traffic before forwarding the PPPoE payload to a PPPoE server. The protocol stack is shown in Fig. 14.

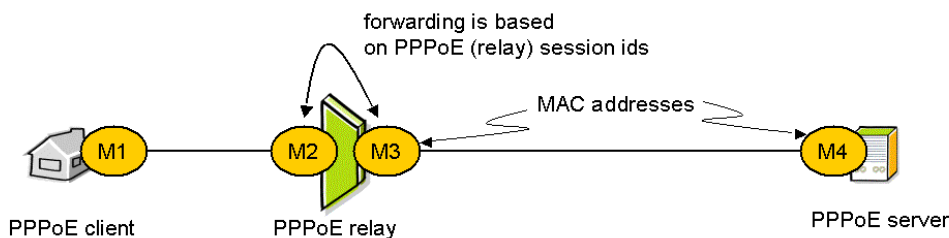
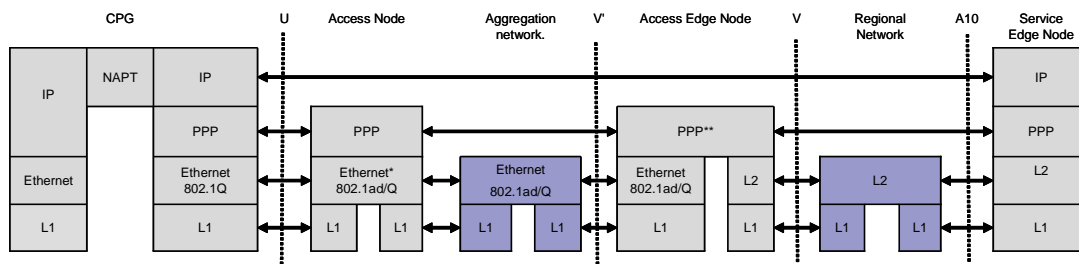


Figure 13: PPPoE relay



* MAC address is changed.

** PPP session is either terminated in the AEN or tunnelled to the SEN

Figure 14: Protocol Stack for Relaying PPP Traffic in the Access Node

PPP Processing

A more radical approach to IPoPPPoE traffic, shown in Fig. 15, is to fully process the PPP sessions at the IP forwarder, either by L2TP tunnelling towards an EN, as shown in Fig 16, (IP FW is then a LAC, for PPP wholesaling), or by terminating and aggregating the PPP sessions, as shown in Fig. 17 (IP FW then performs PTA, for IP connectivity). There is a full separation at L2 between users and aggregation network for this traffic.

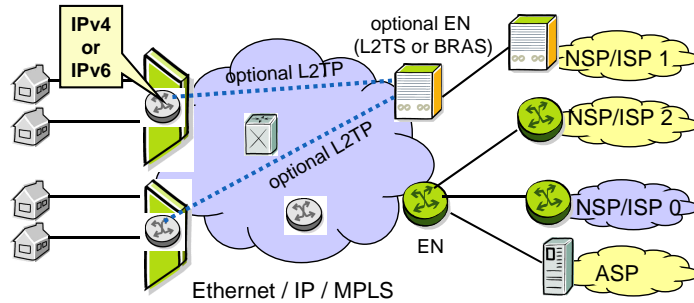


Figure 15: IPoPPPoE traffic handled in IP forwarder (LAC/PTA)

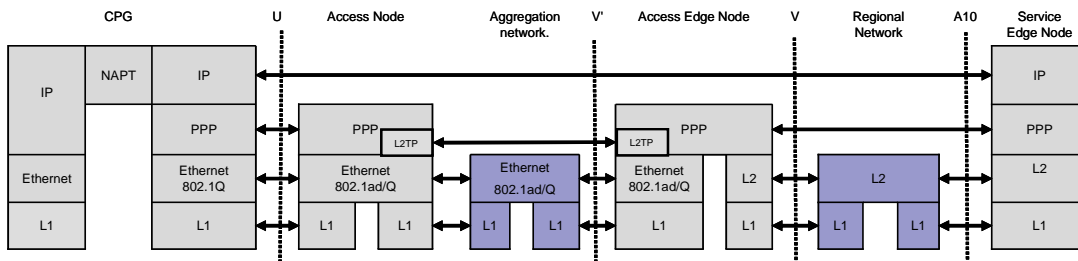


Figure 16: Protocol Stack for L2TP Access Aggregation (LAC)

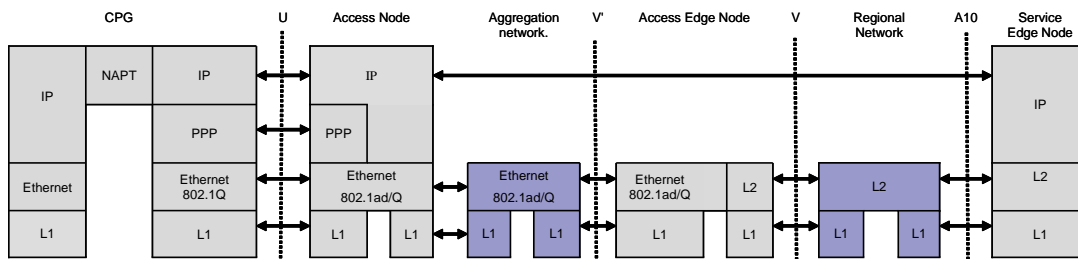


Figure 17: Protocol Stack for PPP Terminated Aggregation (PTA)

Which Option?

In MUSE L2 switching of PPP has been identified as interesting in the near term by most operator partners. It is simple – there is no need for the access node to do PPP manipulation - and it allows the re-use of already deployed BRAS's thus enabling migration. Therefore L2 switching of PPP is recommended.

PPPoE relay routing for the retail business model received almost the same interest from most operator partners in MUSE. Therefore, PPPoE relay is regarded as a useful option.

There is little interest in LAC/PTA option amongst the operator partners in MUSE. The drawback is the complexity and lack of flexibility of the option. It is included here for completeness but is not recommended by MUSE.

In order to handle IPoE traffic, three options were selected in DA2.2: IP forwarding (IP transport service), IP routing for application wholesale, and IP routing for IP Wholesale.

IP Forwarding (IP Transport Service)

The first is for the NAP to provide IP transport service. Fig. 18 shows the basic network scenario for the switched IP transport scenario. In this case the NAP transports IP packets from the IP forwarder, being in the above example the access multiplexer, to the appropriate ISP/NSP/ASP. For doing so the NAP installs appropriate service connections between the IP forwarders and the peering points to the service providers.

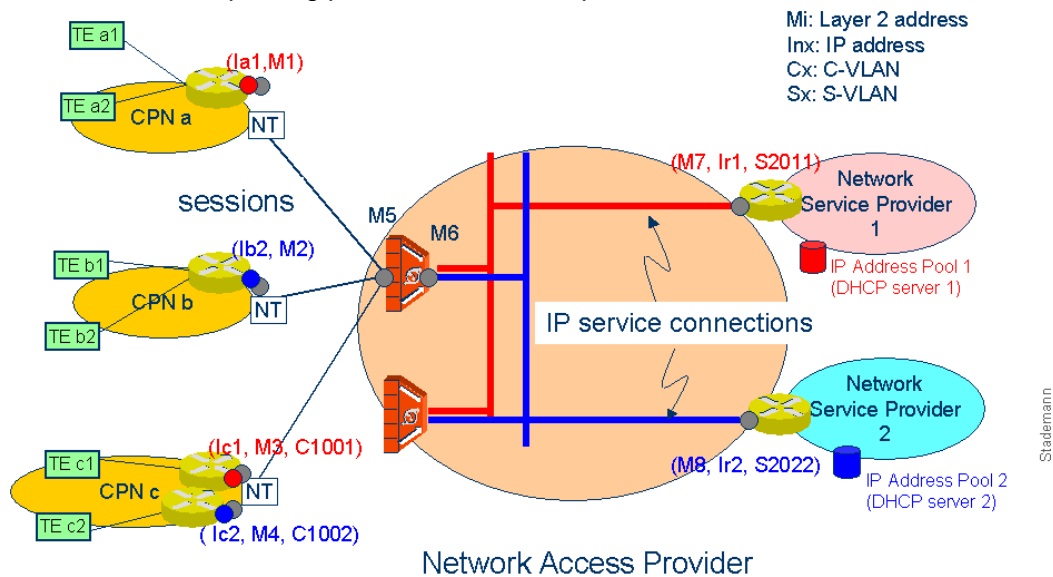


Figure 18: Data plane example for the basic scenario with NAP providing IP services

IP Sessions are characterized by the MAC and associated IP address in the CPN and optionally also by a C-VLAN when service multiplexing is used. Optionally also additional data like DSCP code points, .1p bits or UDP ports may be used to identify sub-flows within a single IP session.

The IP forwarder binds IP sessions on the CPN side to the network side IP service connections based on the information shown in Table 2.

The corresponding U interface protocol stack is shown in Fig. 19.

Session (DSLAM MAC= M5)					IP Service Connection (ISC) (DSLAM MAC= M6)		
Phys. Port	C-VLAN	IP(user)	Layer 2 Address (user)	optional data	S-VLAN	MAC (edge node)	optional data
a	-	1a1	M1		2011	M7	
b	-	1b2	M2		2022	M8	
c	1001	1c1	M3		2011	M7	
c	1002	1c2	M4		2022	M8	

Table 2: Binding of IP sessions to service connections in the IP forwarder

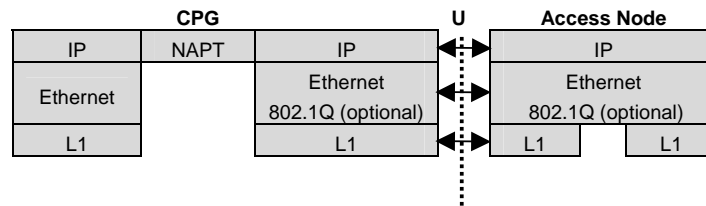


Figure 19: U Interface Protocol Stack for NAP Provided IP Services

IP Routing for Application Wholesale

The second option proposed is for the NAP to provide routed IP service for application wholesale as depicted in Fig. 20.

The NAP and NSP0 offer an IP network service to the end customers. In an access network with routed IP there is no end-to-end L2 connectivity between the CPG and the AEN. The CPG will therefore be connected via L2 to the nearest IP forwarder in the network. The protocol stacks for this option are shown in Fig. 21.

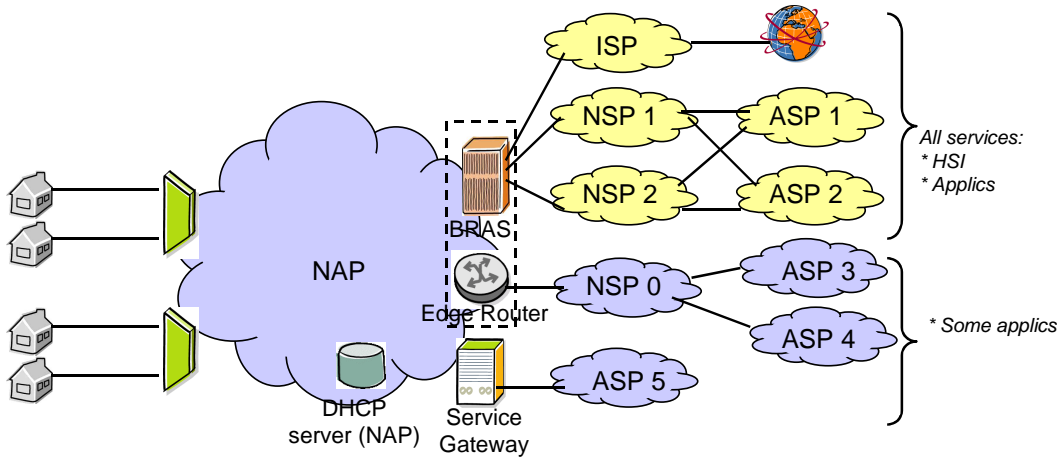


Figure 20: Most applicable business scenario for routed IP in the NAP network

DA2.2 [2] proposes two approaches in order to handle IPv4/IPv6 subnetting :

- VLAN aggregation solution (RFC 3069)
- LAN aggregation solution

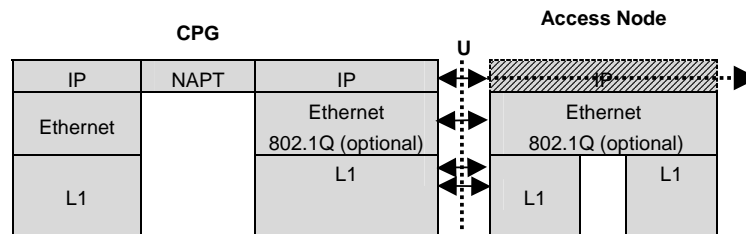


Figure 21: U-Interface Protocol Stack for Routed IP in the NAP Network

IP Routing for IP Wholesale

The third option of IP routing for IP wholesale is identical to the second, except that IPoE traffic for retail and wholesale users must be supported.

Which Option?

IP forwarding has been identified as interesting in the near term by most operator partners in MUSE. Its advantages are simplicity of deployment (maximum re-use of existing deployments, lower management complexity than IP routing for some operator partners). The centralized addressing scheme has the widest preference (for efficiency). Therefore MUSE recommends IP forwarding with centralized addressing scheme.

IP routing for retail is also of interest to most operator partners in MUSE (albeit sometimes longer term and with some reservations). Possible advantages over IP forwarding can be

simplicity of IP routing in terms of management and suitability for peer-peer communication. There are reservations about scaling (unless IP6 is used), configuration and complexity of having IP routing in many nodes. MUSE recommends IP routing for retail.

There is little interest in IP routing for wholesale amongst the operator partners of MUSE because of its drawbacks complexity and lack of flexibility. IP routing is included here for completeness but is not recommended by MUSE.

3.1.3 Access Node to Access Edge Node Interface (V')

There are a number of options for the V' interface depending on the business model and network model being used. The protocol stack used across the V' for the Ethernet network model is shown in Fig. 11. For the IPoPPPoE options the V' interface protocol stacks are shown in: Fig. 14 for Relaying PPP, Fig. 16 for L2TP and Fig. 17 for PTA. For IPoE the protocol stack is shown in Fig. 22.

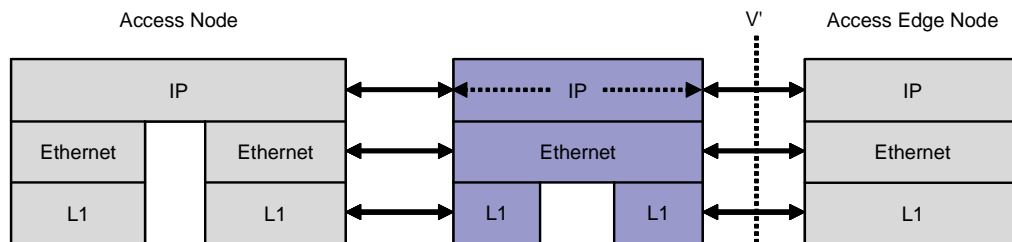


Figure 22: V'- Interface Protocol Stack for IPoE

3.1.4 Access Edge Node to Regional Network Interface (V) or Regional Network to Service Edge Node (A10)

There are a number of options for V and A10 interfaces depending on the business model being used. DA2.2 Section 2.3 defines a number of business models which from the point of view of different interfaces gives rise to 3 particular variants of the reference model in Fig. 4.

3.1.4.1 V and A10 Interfaces for PPP Wholesale Model

The first variant is shown in Fig. 23. The AEN (for instance a BRAS) of the Access and Aggregation network offers PPP wholesale to NSPs and ISPs either directly or through a Regional Network. The L2 and above interfaces at V or A10 are both IPoPPPoE. The L1 interface at V and A10 may be different, but at L2 and above V and A10 are identical. Fig. 24 shows the protocol stack used across the interface.

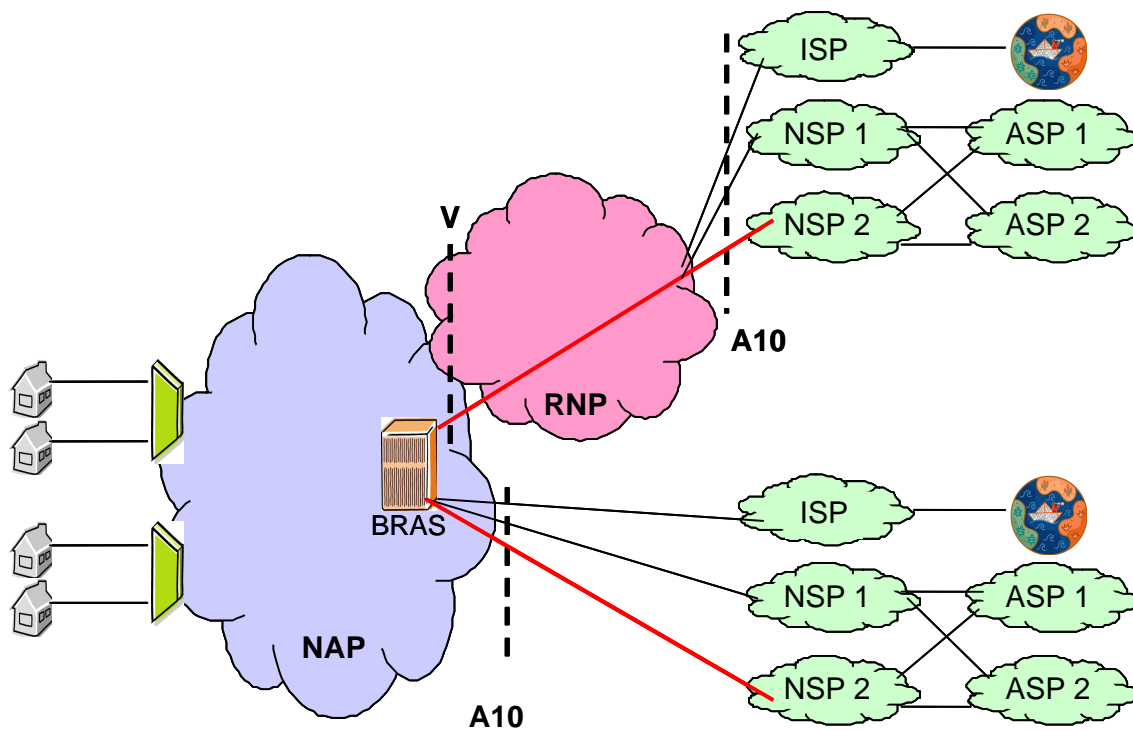


Figure 23: PPP Wholesale

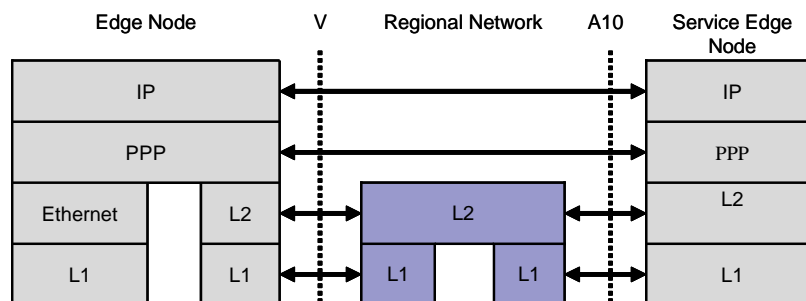


Figure 24: V/A10 Interface Protocol Stack for PPP Wholesale Model

3.1.4.2 V and A10 Interfaces for the IP Wholesale Model

The second variant is shown in Fig. 25. A router of the NSP network interfaces to an access edge node of the Access and Aggregation network (A10=V), or a router of the regional

network (A10 interface) to transport IPoE traffic. The L2 and above interfaces at V or A10 are both IPoE and DHCP is provided by the NAP. Under the assumption that if the regional network uses MPLS it is confined to the regional network and does not extend into the access or service network domains then the V and V10 interfaces are identical. In this model the protocol stacks are shown in Fig. 26.

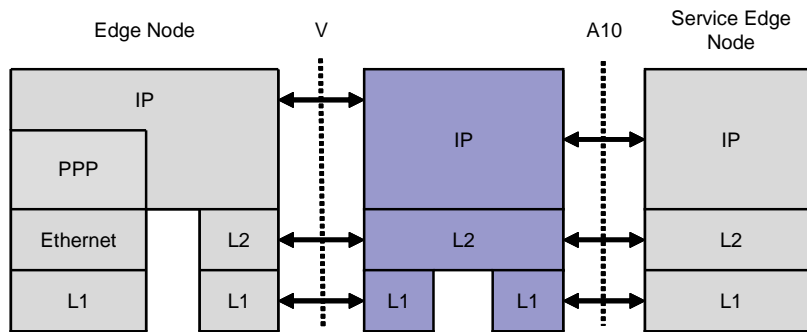
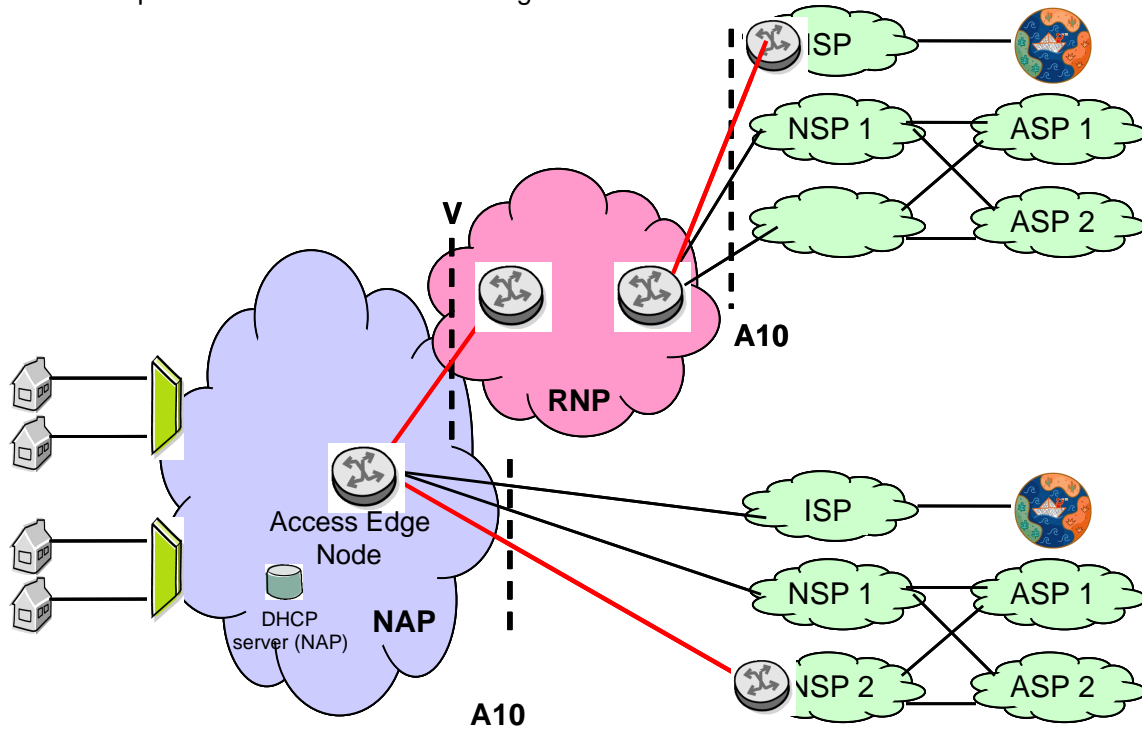


Figure 25: IP Wholesale Model

Figure 26: V/A10 Interface Protocol Stack for IP Wholesale Model

The second layer of the protocol stack in Fig. 26 will be Ethernet 802.1ad in the Ethernet Network model defined in Muse and with optional support of 802.1Q in the IP network model.

3.1.4.3 V and A10 Interfaces for the L2 Wholesale Model

The third variant is shown in Fig. 27. An AEN of the Access and Aggregation network interfaces to a network element of the NSP /ISP either directly or through a L2 regional network in order to provide Ethernet service connectivity or MEF types of services (L2 VPN and Ethernet virtual lines). The V and A10 interfaces are up to L2. At L2 V and A10 are identical but at L1 may be different. The protocol stack for this model is shown in Fig. 28.

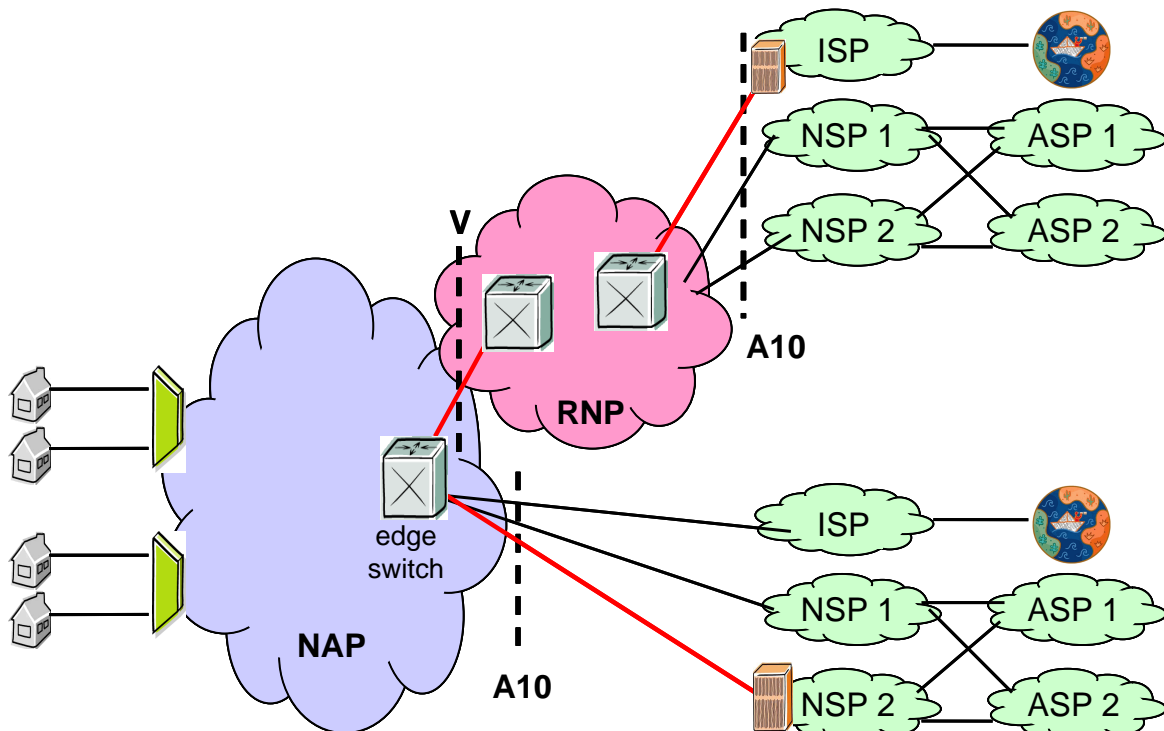
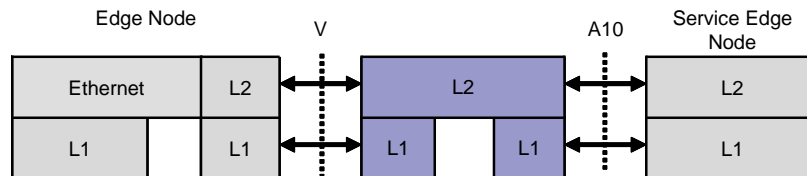


Figure 27: L2 Wholesale Model

Figure 28: V/A10 Interface Protocol Stack for L2 Wholesale Model

3.2 Management Interfaces

CPs have the role of setting up the end to end connectivity between CPGs and the SENs. The Packager provides information about the nature of the connection that is required across the Q_p interface. A network management server in the CP domain using the information from the Packager communicates with the management entities in the Access Network, Regional Network and SEN. The first stage in this is a management function that provisions the connection between the AN and the SEN. Provisioning sets up the potential path or paths through the networks that are required to provide the end user with the services they may choose to use. At this stage there may be no CPG connected or, if it is, no active applications (IP flows) in use. When a CPG is connected then auto-configuration of the CPG takes place. L1 and L2 configuration is achieved by embedded management capabilities and, following the AAA process (see section 3.3) to establish L3 capability, the CPG establishes contact with the Auto-Configuration Server (ACS) in the CP Domain to configure more advanced and higher layer features. The setting up of application flows on a session by session basis is the job of the control plane interfaces which are described later.



3.2.1 Connectivity Provider to Access Network Manager Interface (Q_A)

The access network manager in Fig. 5 is a generic term to cover the management functions that are required to provision and operate connections across the access and aggregation network. In practice the access network manager consists of network management functions and network element functions. Generally, the element management functions are specific to the technology being managed and so the three types of node would have their own element manager and each element manager would manage multiple nodes. This decomposition reveals several interfaces. The interfaces between element managers and their respective elements are usually proprietary. The interfaces between the element managers and the access network manager may well be standard interfaces but, since they are all within the single (access) domain, they are not regarded as open interfaces in the context of MUSE. Further discussion of the management architecture for the access and aggregation network can be found in deliverable DTF1.3 [8]. DTF1.3 also describes the functionality required in the flow-through management chain for the FCAPS functional areas. MUSE has not specifically defined the Q_A interface but the interface must support the functions discussed in DTF1.3.

3.2.2 Connectivity Provider to Regional Network Manager Interface (Q_R)

The regional network manager in Fig. 5 is a generic term to cover the management functions that are required to provision and operate connections across the regional network. In practice the access network manager consists of network management functions and network element functions. The discussion in DTF1.3 also applies to the management of the regional network.

3.2.3 Connectivity Provider to Service Edge Node Interface (Q_S)

Similarly, DTF1.3 has not specifically defined the Q_S interface but Q_S will need to support the transport management functionalities described in TF1.3. It should be noted that application specific functionality in the SEN would be managed by the application provider.

3.2.4 Connectivity Provider (ACS) to CPG Interface (Q_C)

The Q_C interface¹⁰ is used to exchange management information between the CPG and the ACS server in the CP's domain after a network connection has been established. The ACS can be used for following types of management operations: auto-configuration/dynamic service provisioning, firmware/software image management, status and performance management and diagnostics.

¹⁰ Note that in TISPAN this interface is denoted as e3 and the ACS would contain the CPE Configuration Function (CPECF)

The communication protocol is based on the protocol stack and procedures described in DSLF document TR-069 [9]. Fig. 29 shows the Q_c protocol stack which, of course, is transported over the U interface to the CPG. The use of SSL/TLS is recommended, although the protocol may also be used directly over the TCP/IP connection.

CPE/ACS Management Application
RPC Methods
SOAP
HTTP
SSL/TLS
TCP/IP

Figure 29: ACS to CPG Management Protocol Stack

The ACS can read or write parameters in the CPG by means of a defined RPC method. Also file transfer and CPG initiated notifications are defined by this method. Both the CPG and the ACS may initiate a connection establishment, avoiding the need for a persistent connection to be maintained between each CPG and an ACS. The CPG is aware of only one ACS with which it can connect. The ACS may hand over a CPG to another ACS by explicitly altering the ACS contact information and authentication information.

3.2.5 Packager/NSP/ASP interface to Connectivity Provider (ACS) (Q_p)

The ACS and network manager have been attributed to the Connectivity Provider in order to make it possible for multiple Packagers and associated service/application providers to share management platform resources. ACS and network manager northbound interfaces have to be defined towards the Packagers and the NSPs/ASPs. The Packager is responsible for ensuring that only associated NSPs/ASPs have access to the management platform and that they can configure/modify parameters that belong to their own domain. NSPs/ASPs may have an interface directly with the ACS to manage service specific parameters (not shown in the Fig. 5). This interface has not been studied in MUSE but is currently being progressed in the DSL Forum.

3.3 Control Interfaces

The reference model in Fig.6 shows several control reference points. A clearer picture of what is happening in the control space can be obtained by realising that there are two levels of control: connection control and application control. The reference points e1-e5, a1-a4, C_{m1}, C_{m2} and C_{m3} give rise to interfaces that are concerned with the connection control. In particular, the e1-e5 and a1-a4 reference points are concerned with AAA and IP address assignment functionality and are taken from the ETSI-TISPAN Network Attachment Subsystem (NASS) [11]. The approach to AAA and IP address assignment is described in reference [2]. The other reference points are to do with application level control of IP flows and the resources required to deliver the required QoS for the IP flow on a session by session basis. The interfaces at these reference points are based on the ETSI-TISPAN Resource and Admission Control Subsystem (RACS) [10]. In addition, the reference point A_{ctrl} has been added to account for applications that are not based on SIP signalling. In practice it is likely that the A_{ctrl} interface will be the same as the G_q interface.

3.3.1 CPE to AMF Interface (e1)

This interface enables the CPE to initiate requests for IP address allocation and possible other network configuration parameters in order to access to the network. These requests are received by the Access Management Function (AMF). The AMF translates network access requests issued by the CPE.

It forwards the requests for allocation of an IP address and possibly additional network configuration parameters to the NACF and returns addresses and parameters to the CPE.

The AMF forwards requests to the User Access Authorisation Function (UAAF) to authenticate the user, authorize or deny the network access, and retrieve user-specific access configuration parameters.

3.3.2 AMF – UAAF Interface (a3)

This interface allows the AMF to request the UAAF for user authentication and network subscription checking. As shown in Fig. 4 this interface is not an open interface because it is internal to the NAP. However, it is included here in case the NAP does not provide a UAAF proxy in which case the e5 interface does not exist and there is a direct connection between the AMF and the UAAF.

The User Access Authorisation Function (UAAF) performs user authentication, as well as authorisation checking, based on user profiles, for network access. For each user, the UAAF retrieves authentication data and access authorization information from the user network profile information contained in the Profile Database Function (PDBF). The UAAF also collects accounting data for user charging for each CPE authenticated by NASS. The PDBF is the functional entity that contains user authentication data (user identity, list of supported authentication methods, key materials...) and information related to the required network access configuration: these data are called "user network profile".

The AMF inserts in the signalling with the UAAF the Line ID of the line for which authentication is taking place.

NOTE: The AMF acts as a RADIUS client if the UAAF is implemented in a RADIUS server. The role of the AMF when using DHCP requires further studies and depends on which solution will be standardized for implementing authentication procedures.

3.3.3 AMF – NACF Interface (a1)

This interface allows the AMF to request the Network Access Configuration Function (NACF) to allocate an IP address to end user equipment as well as provide other network configuration parameters such as address of DNS server(s), address of signalling proxies for specific protocols (e.g. address of the P-CSCF when accessing to an IMS). Requests for IP address allocation and network configuration parameters are either in the form of a DHCP or PPP request.

It is assumed that the IP edge in the transport plane includes an access relay function that either:

- Terminates the PPP connection and provides the inter-working with the interface to the network attachment subsystem e.g. using an AAA protocol (RADIUS or Diameter).
- Act as a DHCP relay between the DHCP client in user equipments and the DHCP server in the network attachment subsystem.

In both cases, before sending a request to the network attachment subsystem, the relay function may add network location information to the information received from the user equipment.

This interface enables the user equipment to provide user credentials (password, token, certificate...) to the Network Attachment Subsystem (NASS) in order to perform network access authentication. It may also enable the NASS to provide authentication parameter to the CPE to perform the network authentication when mutual authentication procedure is required. Based on the authentication result, the AMF authorizes or denies the network access to the user equipment.

The NACF interacts with the UAAF to register the association between the IP address allocated by the NACF and the Line ID.

NOTE: DHCP servers or RADIUS servers are typical implementations of the NACF.

3.3.4 NACF – CLF Interface (a2)

This interface allows the NACF to register in the Connectivity Session Location Function (CLF) the association between the allocated IP address and the user identity as well as related location information i.e. access transport equipment characteristics, line identifier (Line ID), IP Edge identity, etc. The CLF registers the association between network location information received from the NACF and geographical location information. The CLF may also store the identity of the user/ CPE to which the IP address has been allocated (information received from the UAAF), as well as user preferences regarding the privacy of location information.

The CLF responds to location queries from service control subsystems and applications. The actual information delivered by the CLF may take various forms (e.g. network location, geographical coordinates, post mail address ...), depending on agreements with the requestor and on user preferences regarding the privacy of its location.

The CLF interfaces with the NACF to get the association between the IP address allocated by the NACF to the end user equipment and the Line ID .

The CLF also registers user network profile information (received from the UAAF at authentication) to make this profile information available to the RACS at authentication of the CPE.

Where shown in Fig. 6 a2 is not an open interface but is included here to make clear the function of the CLF. The CLF contains information that is provided from management systems.

3.3.5 UAAF – CLF Interface (a4)

This interface allows the CLF to register the association between the user identity and the user preferences regarding the privacy of location information provided by the UAAF. It is also used to register user network profile information (QoS profile).

Again, as Fig. 6 shows this is not an open interface but is shown for completeness.

3.3.6 CLF and RACF Interface (e4)

This interface allows the RACS to retrieve network location information from the CLF (e.g. the address of the physical node through which the user can be reached) in order to determine the amount of available network resources. The e4 reference point allows the RACS also to retrieve user network profile information from the CLF in order to take them into account when processing resource allocation requests. The information exchanged on the e4 interface is the binding between the Line ID, the assigned IP@ and the ID of the IP edge, user network profile information in order to take them into account when processing resource allocation requests.

3.3.7 CLF and AF Interface (e2)

This interface enables applications and service control subsystems to retrieve from the CLF network location information. The form of location information that is provided by the CLF depends on the requestor.

3.3.8 UAAF to UAAF-proxy Interface (e5)

This interface provides the signalling between the UAAF and the UAAF-proxy.

3.3.9 AAA and IP Address Assignment Protocols

As with the evolution of data plane protocols, it is expected that PPP will gradually be replaced by DHCP, but PPP is not going to disappear over night and is very likely to remain an important authentication technology for the coming years. So we expect to see: PPP (RFC 1661), PPPoE (RFC 2364), PPPoA (RFC 1483) for some time.

For the future MUSE proposes the use of a one step AAA (including IP address assignment) process using a combination of DHCP, Radius and Extensible Authorisation Protocol (EAP). For the wholesale IP business model the DHCP server is in the Network Service Provider Domain with a DHCP relay in the Network Access Provider Domain. Similarly the Radius server is in the Connectivity Provider Domain with a Radius proxy in the Network Access Provider Domain.

Fig. 30 illustrates the end to end message flows. The two protocols, EAP and DHCP, operate across the e1 Interface. DHCP operates across the a1 interface and Radius across the e5 interface. Fig. 30 also shows the positioning of the appropriate NASS functions.

3.3.10 CPG to Multicast Control Functions Interfaces (C_{m1} , C_{m2} and C_{m3})

The reference model in Fig. 6 shows the several control plane reference points required between the customer domain and the access network provider domain (C_{m1}), the access network provider domain and the regional network domain (C_{m2}), and the regional network provider domain and the application provider domain (C_{m3}) which hosts the multicast sources.

The MUSE architecture focuses on the control connection between the customer domain and the MUSE access and aggregation domain. IGMPv2 and, in the near future, IGMPv3 is the most common group management control used as a signalling protocol. Therefore, MUSE recommends that IGMPv2 or v3 is the signalling protocol used between the customer domain and the access node.

The signalling protocol purpose is to allow customers to select (S,G) if IGMPv3 is used, where G(Group) is the multicast IP@ which corresponds to the stream and S(Source) is the unicast IP@ the stream is coming from, or where IGMP2 is used (*,G) corresponding to a channel they want to access.

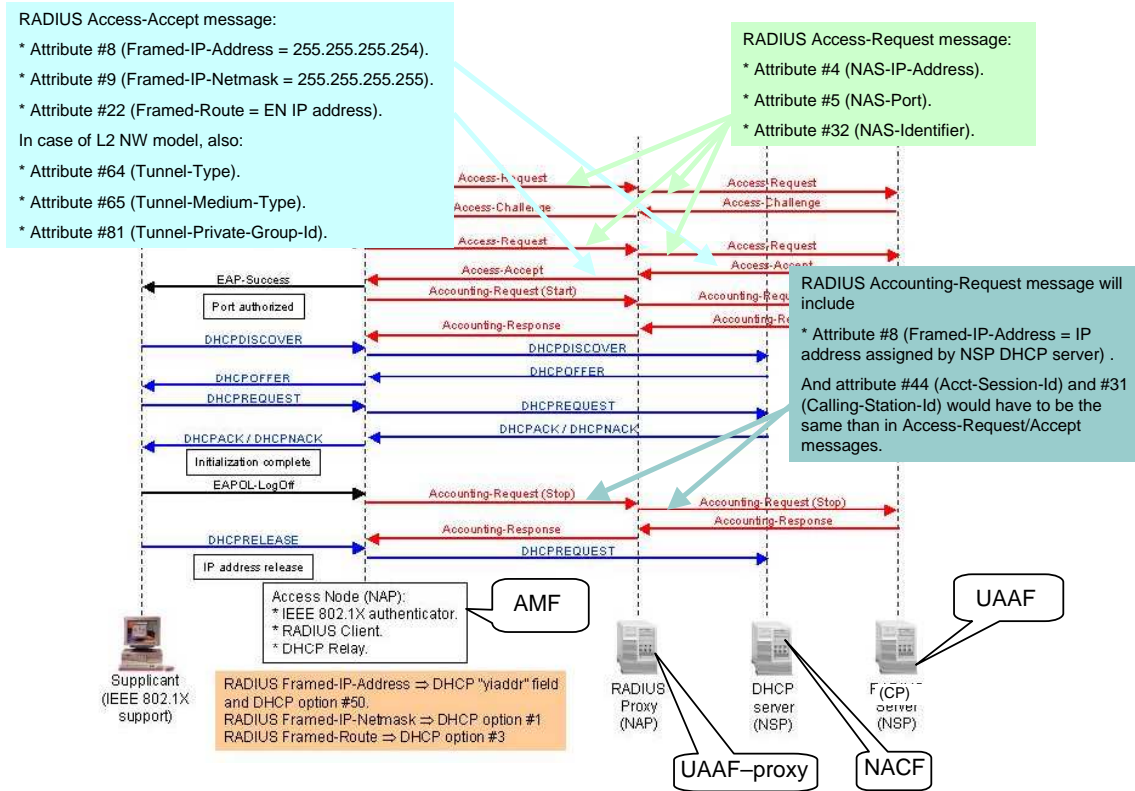


Figure 30: One Step AAA process, DHCP Relay in the Access Network

Multicast aims at optimizing the bandwidth consumption by replicating streams at several points to avoid conveying the same stream several times. To apply this mechanism multicast features are required along the path from customers up to multicast sources which besides corresponds to the data plane path. That is why the Fig. 6 depicts a control connection between each domain the multicast streams pass through.

The following multicast features for a CPG and AN, are extracted from a MUSE multicast contribution to the DSL Forum which adopted the proposed definitions in the WT101 document [12].

Depending on the CPG, two variants of multicast features are possible:

- Bridged CPG: IGMP snooping with proxy reporting. The IGMP snooping function handles multicast replication, and also controls where the packets are replicated to (either port or VLAN). Upon a subscriber issuing a IGMP join to a multicast

group the IGMP snooping function can begin replicating that group's packets to the subscribers physical or logical port in the downstream direction.

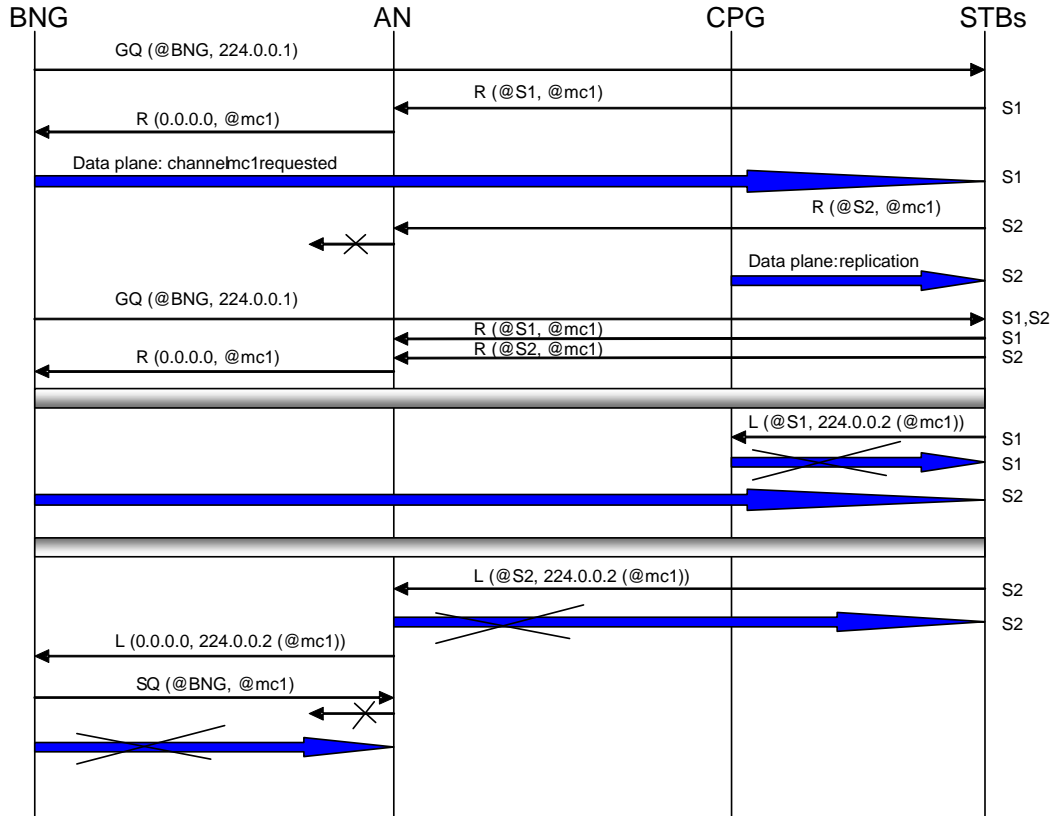
- Routed CPG: IGMP proxy routing

Depending on the AN, two variants of multicast features are possible:

- Bridged AN: IGMP snooping with proxy reporting and IGMP immediate leave
- Routed AN
 - IGMP proxy routing if IGMP termination located at the V interface.
 - IGMP termination (IGMP queries) and PIM DM or SM or SSM.

Note: In IGMPv3 every active receiver of a source group responds to IGMP queries for the group/source. As a consequence an IGMP snooping switch can maintain, on a port by port basis, a complete status on all active receivers, sources, and groups on that port. It is, therefore, possible to speed up the channel change times by the snooping switch explicitly tracking these variables and when the last receiver leaves a source/group pair the switch immediately can remove the associated multicast forwarding entry

To illustrate the control connection between the customer domain and the MUSE access and aggregation domain, the message sequence chart in Fig. 31 depicts a scenario where one customer has two Set Top Boxes (STBs) (S1, S2). The same multicast channel (@mc1) is requested in both STBs. The figure shows the different functions supported with IGMPv2 snooping with proxy reporting and IGMP immediate leave at the AN and IGMP snooping with proxy reporting in the bridged CPE from that port.



GQ: General Query (source @, dest@)
 SQ: Specific Query
 R: Report
 L: Leave

* CPG is a bridge, ie there is no NAPT

Figure 31: Multicast Message Sequence

3.3.11 AF to SPDF (G_q)

In the service provider orientated model for QoS control the CPE communicates via a service level protocol, eg SIP, (which is not part of the MUSE domain) with the IP Multimedia Subsystem (IMS). The IMS initiates a service request via the Application Function (AF) and the AF interacts with the Service Policy Decision Function (SPDF) to make service specific requests for bearer resources and may receive notifications when resources are reserved and released.

The information flow in the interface between AF and SPDF is based on G_q in 3GPP TS29.209 [13] with additions specific for the ETSI-TISPAN IP Connectivity Access Network (IP-CAN) [14], and is named as interface G_q .

The G_q interface is used for network initiated resource reservation, NAT control and service based information exchange between the AF and SPDF. This information is used by the SPDF to initiate resource reservation towards the A-RACF, for gate control and service based policy decisions and to control the NAT functions of the Border Gateway Function (BGF).

The G_q requirements are directly derived from requirements of R_q (SPDF to RACF) and I_a (SPDF to BGF) reference points. However it should be noted that the G_q reference point is not a simple aggregation of functions deriving into two separate information flows for R_q - related and I_a - related requests. The G_q interface also allows for reservations relevant to R_q and I_a to be requested by AF's as a single request, which the SPDF can then split into separate requests and coordinate accordingly depending on the service request.

3.3.12 SPDF to A-RACF (R_q)

The SPDF has a view of the network segments used to provide end-to-end service. It relates the QoS requirements required for the request from the AF to the required end-to-end network connection and where appropriate apportion QoS requirements to each network segment. The SPDF communicates via the R_q interface with the A-RACF. The A-RACF has knowledge of the topology of the access network, the total resources available at each node in the access domain and their current usage from the RDB (Fig.5). A-RACF works at the level of controlling IP application flows at IP-aware nodes. These nodes are in general the IP ingress points at the edges of the access network. The control is exerted by session admission control and shaping at the input to pre-provisioned pipes across the access network.

The R_q interface is used for QoS resource reservation information exchange between the SPDF and the A-RACF. The SPDF issues requests for resources in the access network, indicating IP QoS characteristics. The A-RACF uses the IP QoS information to perform admission control and indicate to the SPDF via the R_q interface its admission control decisions.

3.3.12.1 Information exchanged via the R_q interface

The SPDF provides the following information to the A-RACF to be used as a basis for the resource reservation.

Each resource reservation shall be expressed in terms of:

- An application identifier, allowing unique identification of the application instance on behalf of which individual resource reservations have been established.
- A session identifier, representing a group of media flows that belong to the same application session. Resource management services shall provide atomicity at the level of these application sessions.

- Each application can have multiple independent, yet simultaneously active service sessions.
- A priority level indication (e.g. AF may use this for Emergency Services).
- Per media flow in an application session, the resource reservation shall be expressed and established in terms of a traffic classification and resource requirement description.
- Traffic classification shall provide concise characteristics of the traffic for which resources are reserved (address realm ID, source and destination IP address and protocol version, protocol, source and destination port). Wildcarding of address and port parameters shall be supported.
- A bandwidth resource requirement description is provided for every individual media flow. Bandwidth resource requirements express the bandwidth-related QoS characteristics requested for the media flow.

3.3.13 SPDF to BGF (I_a) Interface

This is the interface between SPDF and C-BGF which supports the following requirements for:

- Control of NAPT-PT, Hosted NAT traversal and Gating
 - Request of NAPT-PT binding (two terminations, each containing an IP address, port and IP version) to receive and transmit the media flows; information about the allocated bindings must be returned to the requester.
 - Indicate, in NAPT-PT binding request, remote source and destination media parameters for each media flow, including possible wildcarding of specific media parameters (in case the information is not known by the controlling node).
 - Indicate, in NAPT-PT binding request, IP address/port latching for specific terminations (if the information cannot be retrieved from signalling data, the data is known to be incorrect etc).
 - Indicate, in NAPT-PT binding request, media transport protocol (RTP, T.38, MSRP etc) for each media flow in order for the C-BGF to be able to perform protocol specific functions (eg dual-port reservation for RTP/RTCP, proper statistics collection etc).
 - Indicate, in NAPT-PT binding request, if media flow is uni- or bi-directional (in case of uni-directional, also indicate the specific direction).
 - Request mid-session modification of media parameters, including possible request for new IP address/port latching.
- Bandwidth control
 - Request allocation of bandwidth resources needed for a specific media flow.
 - Indicate, in the bandwidth allocation request, bandwidth policing information.
 - Request mid-session bandwidth modification.
- QoS marking
 - Indicate QoS marking values (eg Diffserv/DSCP) for each egress media flow.

- Usage metering and statistics reporting
 - Report media flow specific usage metering information (kbytes of sent data etc), when flow is released and during mid-session, if requested.

3.3.14 A-RACF to RCEF (R_e)

The R_e interface is between the A-RACF and the Resource Control Enforcement Function (RCEF) in the AEN. As shown the R_e reference point is not an open interface because it lies in one business domain. It is described here to complete the overall control picture. The RCEF performs policy enforcement functions under control of the A-RACF. The RCEF enforces the policies defined by the access provider. Those policies are provided by the A-RACF through the R_e reference point. Unidirectional micro-flows are specified by the A-RACF towards the RCEF in terms of a flow classifier including the standard 5-tuple (source IP address, destination IP address, source port, destination port, protocol). Elements of the 5-tuple that are unknown to the A-RACF may be wild-carded by the AF in the instructions to the SPDF.

3.3.15 A-RACF to RCEF_a (R_a)

The R_a interface from the A-RACF to the access node is identified in ETSI-TISPAN but as yet has not been defined. In Fig. 6 the function RCEF_a is shown. This does not exist in ETSI-TISPAN at present and has been introduced in MUSE to enable R_a to be defined. It is intended to have similar functionality to RCEF. As MUSE develops this innovation it is intended to contribute it to the development of ETSI TISPAN specifications.

R_a can be regarded as optional, control interface between the RACF and the RCEF_a only for policing. The flow policing mechanism could be based on source & destination IP addresses, port numbers & protocol id. The interface between the resource mediation system and the network elements should support the policing function by providing the necessary parameters for the starting and stopping of the policing function.

The admission control function when there is not enough resource for a service request is in the acknowledgement to the service request itself from the IMS to the CPE. A negative acknowledgement means that the flow would not be set-up and a positive acknowledgement means that the resource is reserved for that flow and the CPE can set up the flow. Note: The CPE is a trusted node, since no policing is done at the AN, if R_a is not used.

As ETSI-TISPAN RACS is intended to work at the level of controlling application IP-flows an interface to the access node is only meaningful if the access-node is IP aware. The Ethernet aggregation model in MUSE does not envisage IP aware access nodes and so this interface only applies to the IP network model. Also, the use of multiple services over each customer access line means that flow control will need to be exerted at the CPG for the upstream traffic to avoid congestion problems over the first mile technology.

It is proposed that there is a need to develop an interface between the RACS and the CPG which here we will call R_c (Note: a corresponding reference point is not shown in Fig. 6). The purpose of the interface would be to control flows in the upstream direction to prevent deterioration of QoS due to the bandwidth restriction of the first mile technology. It would do this by enabling admission control (especially for non-IMS based applications) for new flows and policing of existing flows. In practice R_c may be very similar to R_a . Indeed, given that the information that needs to be conveyed across the interface both R_c and R_a may be very similar to R_e .

4 Conclusion

This deliverable has outlined the business roles and network architecture options identified in the MUSE project to enable the delivery of multiple simultaneous services to all users from multiple application and service providers. The approach to management and control of network resources has been described. Reference models for the data, management and control plans have been presented and open interfaces identified and described to support flexible business models.

Further work is required to enable the selection of the data plane options to match specific service and deployment scenarios and operational requirements. To complement the management framework described in DTF1.3 more detailed management functions for the L2 and L3 nodes and flow-through interfaces need to be defined. The evolution of the QoS control architecture in ETSI-TISPAN needs to be tracked and influenced to ensure that it is compatible with MUSE.